Segurança e criptografia de dados

ONTAP 9

NetApp
January 17, 2025

Índice

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.

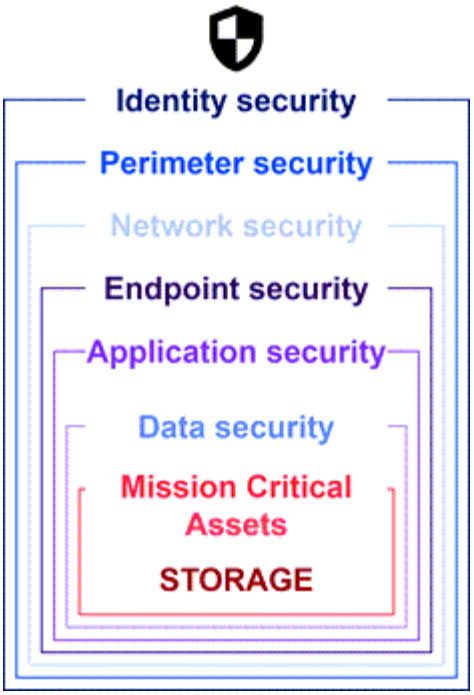
As organizações devem examinar toda a postura de segurança de perímetro, rede, identidade, aplicativo e onde os dados estão no nível de storage e proteger essas camadas. A adoção de uma abordagem centrada em dados à proteção cibernética na camada de storage é crucial no cenário de ameaças atual. Embora 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.

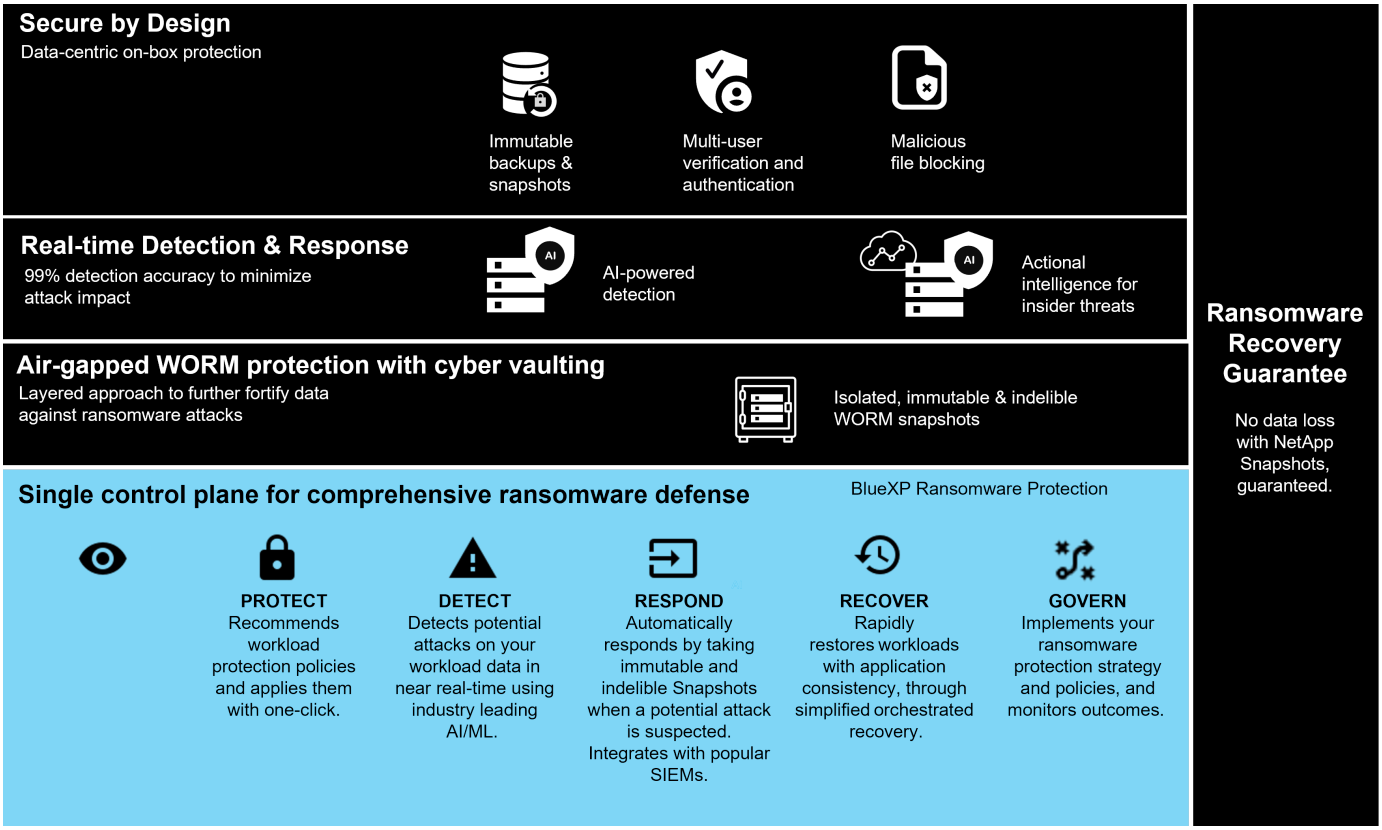
Proteção contra ransomware na camada de dados

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"

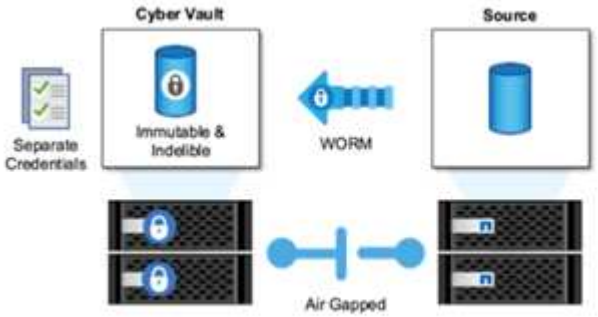
Proteção WORM com uso de cofres cibernéticos

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.

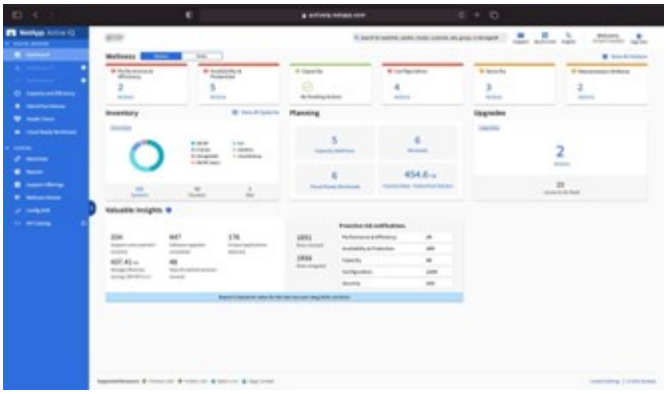
Saiba mais

- "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.

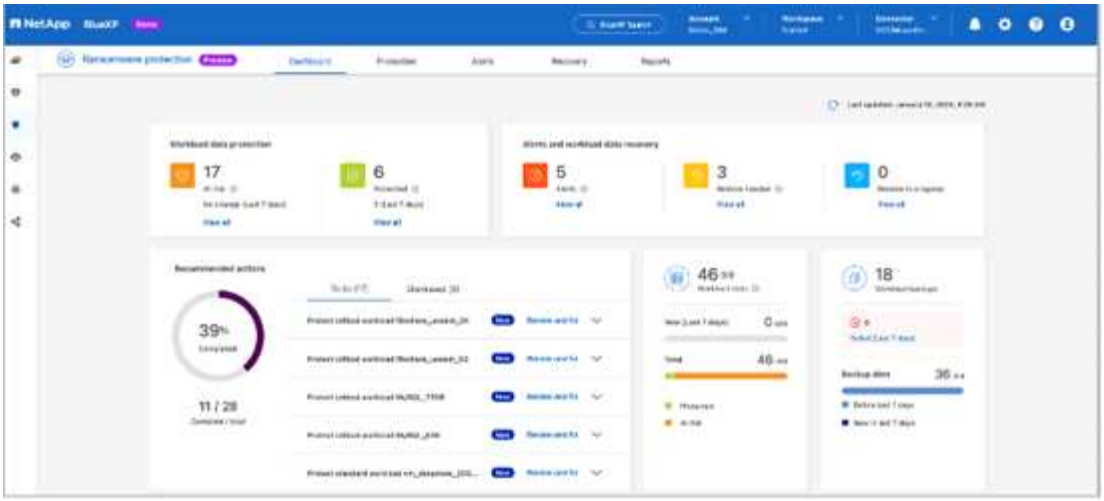
Para ver a proteção contra ransomware do Digital Advisor em ação, "Consultor digital da Active IQ"consulte .

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"
- "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)	✓	✓	✓	✓	✓		
Volumes FlexGroup*	✓	✓	✓	✓			

	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
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 ataques da proteção autônoma contra ransomware com o ONTAP

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 `security anti-ransomware volume attack-detection-parameters modify` o "Referência do comando ONTAP"na .

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. Depois de categorizar o ataque, você pode limpar o aviso e avisos sobre arquivos suspeitos.

Quando o ONTAP deteta uma anomalia, também cria "Um instantâneo ARP" o volume para criar o melhor ponto de recuperação. Os instantâneos ARP são retidos por dois a cinco dias por padrão.

Quando você categoriza um ataque, esses snapshots ARP são excluídos instantaneamente (ONTAP 9.15.1 e anteriores) ou retidos por um período abreviado iniciado pela operação de categorização (ONTAP 9.16.1 e posterior).

A partir do ONTAP 9.11.1, você pode modificar o definições de retenção para instantâneos ARP.

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 ARP for emitido, responda designando a atividade do arquivo de duas maneiras:

- **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

Use o Gerenciador de sistema ou a CLI do ONTAP para responder a atividades anormais.

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 sobre a deteção de atividade de volume anormal, consulte os tipos de ficheiro suspeitos.

   Na guia **Segurança**, selecione a opção para revisar os 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	a. Selecione **Update** e **Clear Suspect File Types** para gravar sua decisão. 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. Esta ação limpa avisos sobre ficheiros suspeitos. Em seguida, o ARP retoma a monitorização normal do volume. Para o ONTAP 9.15.1 e versões anteriores, depois de limpar os tipos de arquivo suspeitos, os snapshots ARP são excluídos automaticamente. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.
Potencial ataque de ransomware	a. Responder ao ataque e "restaurar dados protegidos". b. Selecione **Update** e **Clear Suspect File Types** para gravar sua decisão e retomar o monitoramento ARP normal. Esta ação limpa o relatório de ataque. Não há avisos de tipo de arquivo suspeitos para limpar se você restaurou um volume inteiro. Para o ONTAP 9.15.1 e versões anteriores, depois de restaurar um volume, os instantâneos ARP são automaticamente excluídos. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.

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 -vserver
<svm_name> -volume <vol_name> -dest-path <[svm_name:]vol_name/[sub-
dir-name]>`
```

Exemplo de comando:

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

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:

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

4. Execute uma das seguintes ações com base na avaliação das extensões de arquivo:
   - Falso positivo

Execute o seguinte comando para Registrar sua decisão, adicionando a nova extensão à lista dos permitidos e retomar o monitoramento normal Autonomous ransomware Protection:

```
anti-ransomware volume attack clear-suspect -vserver <svm_name>
-volume <vol_name> [<extension identifiers>] -false-positive true
```

Use o seguinte parâmetro opcional para identificar apenas extensões específicas como falsos positivos:

- `[-extension <text>, … ]`: Extensões de ficheiro

  `clear-suspect`Esta operação limpa avisos sobre ficheiros suspeitos. Em seguida, o ARP retoma a monitorização normal do volume. Para o ONTAP 9.15.1 e versões anteriores, depois de limpar os tipos de arquivo suspeitos, os snapshots ARP são excluídos automaticamente. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.

◦ Possível ataque de ransomware

Responder ao ataque e "Recupere dados do instantâneo de backup criado pelo ARP". Depois que os dados forem recuperados, execute 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 o seguinte parâmetro opcional para identificar apenas extensões específicas como possíveis ransomware:

- `[-extension <text>, … ]`: Extensão do ficheiro

  `clear-suspect`Esta operação limpa o relatório de ataque. Não há avisos de tipo de arquivo suspeitos para limpar se você restaurou um volume inteiro. Para o ONTAP 9.15.1 e versões anteriores, depois de restaurar um volume, os instantâneos ARP são automaticamente excluídos. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.

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>]
   ```

Informações relacionadas

- "KB: Entendendo os ataques Autonomous ransomware Protection e o snapshot Autonomous ransomware Protection".
- "Modificar opções de instantâneos automáticos".

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 e não em outro "Tipos de SVM".

Passos

1. Mostrar todas as definições atuais de instantâneos ARP:

```
options -option-name arw*
```

Para ver a página de manual, introduza `man options` na CLI do ONTAP.

2. Mostrar as definições atuais de instantâneos ARP selecionadas:

```
options -option-name <arw_setting_name>
```

3. Modificar as definições de instantâneos ARP:

```
options -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.
`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.
`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.
`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.

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 .
`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.
`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.

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.

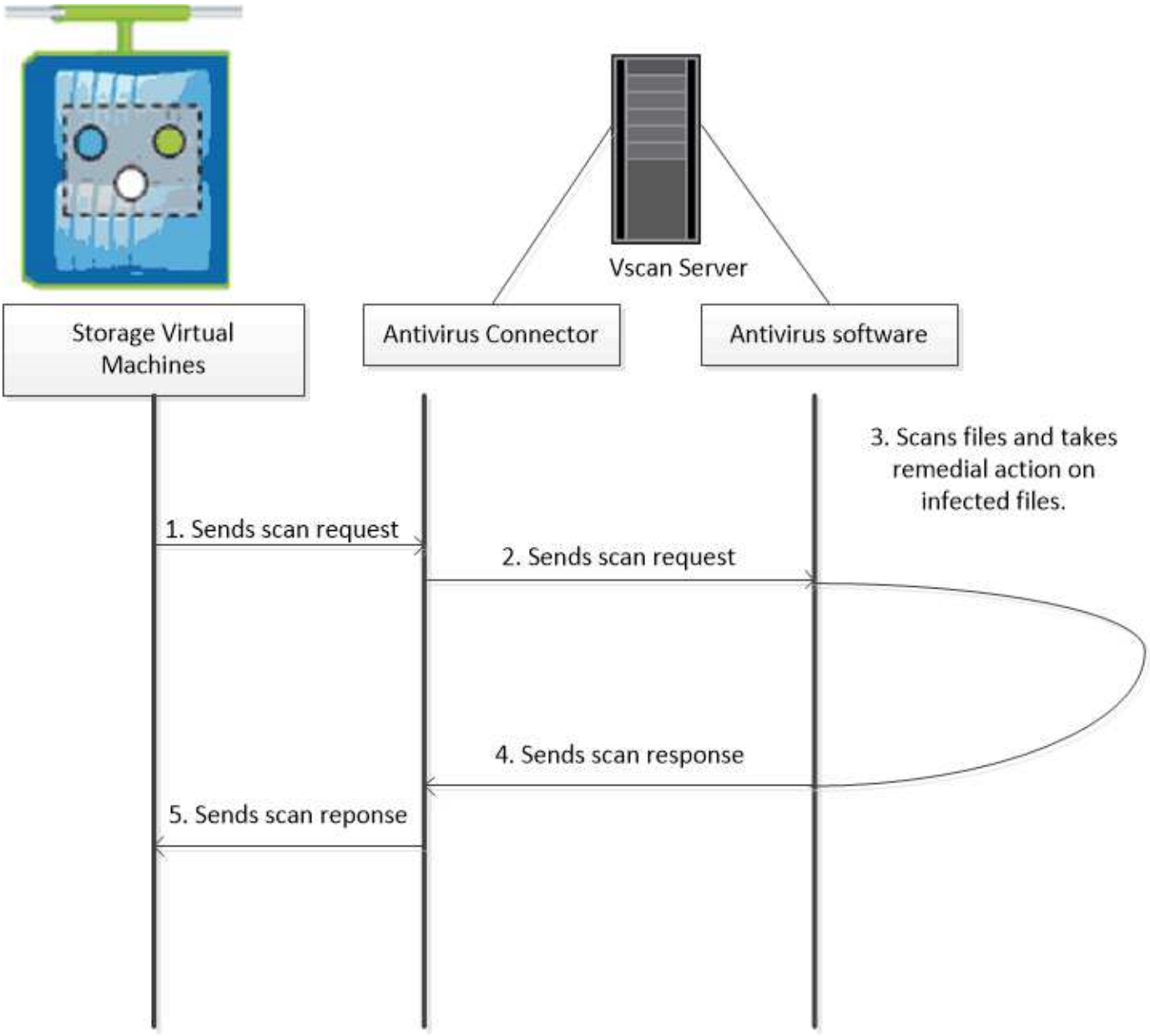
  A verificação no acesso não é suportada para NFS.

- 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.

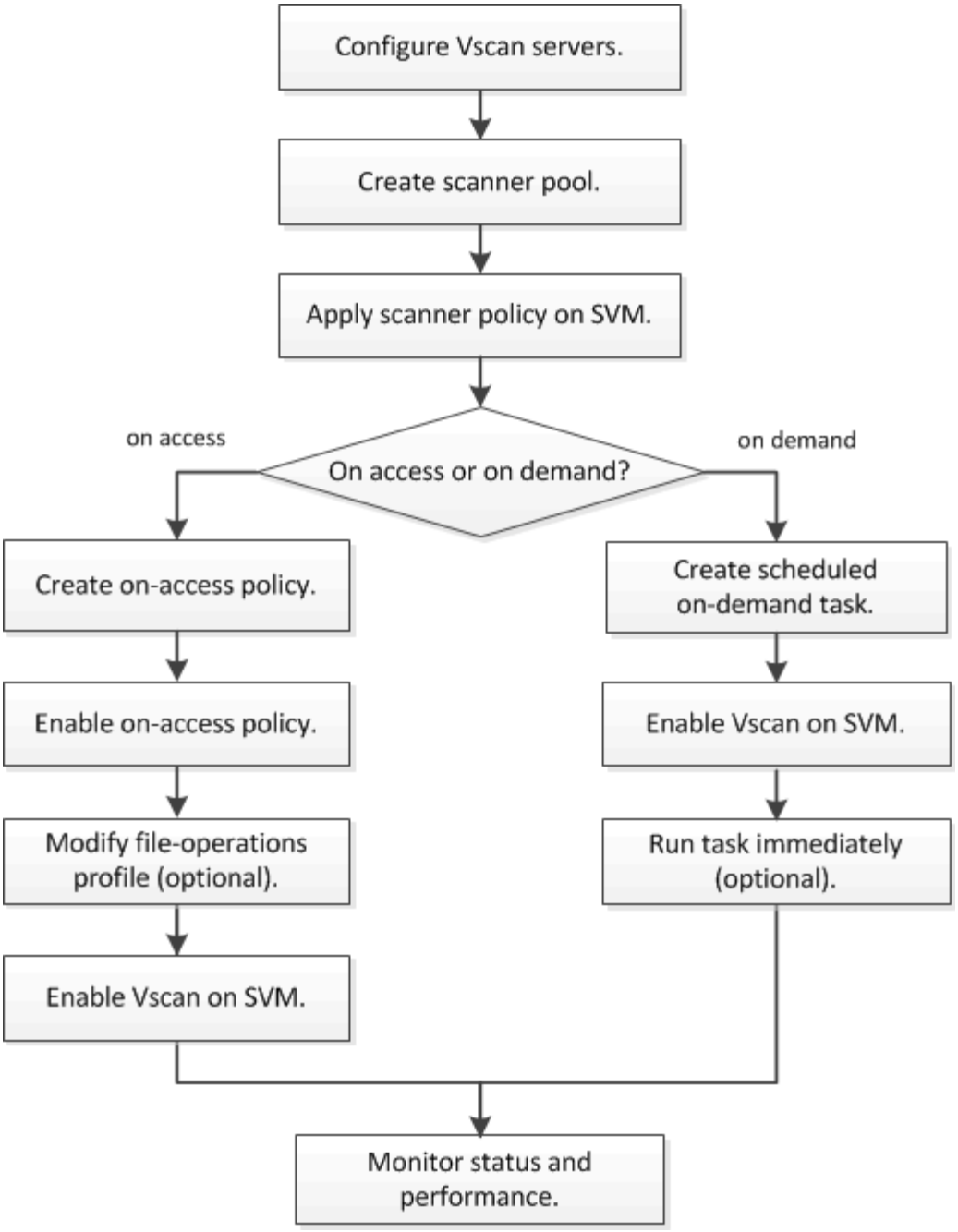
O conetor do antivírus ONTAP, fornecido pelo NetApp e instalado no servidor externo, lida com a comunicação entre o sistema de armazenamento e o software antivírus.



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 `security login role create` e `security login create` no "Referência do 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 `security login domain-tunnel create` o "Referência do comando ONTAP"na .

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 `security login role create` e `security login create` no "Referência do

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 `security login domain-tunnel create` o "Referência do comando ONTAP"na .

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.

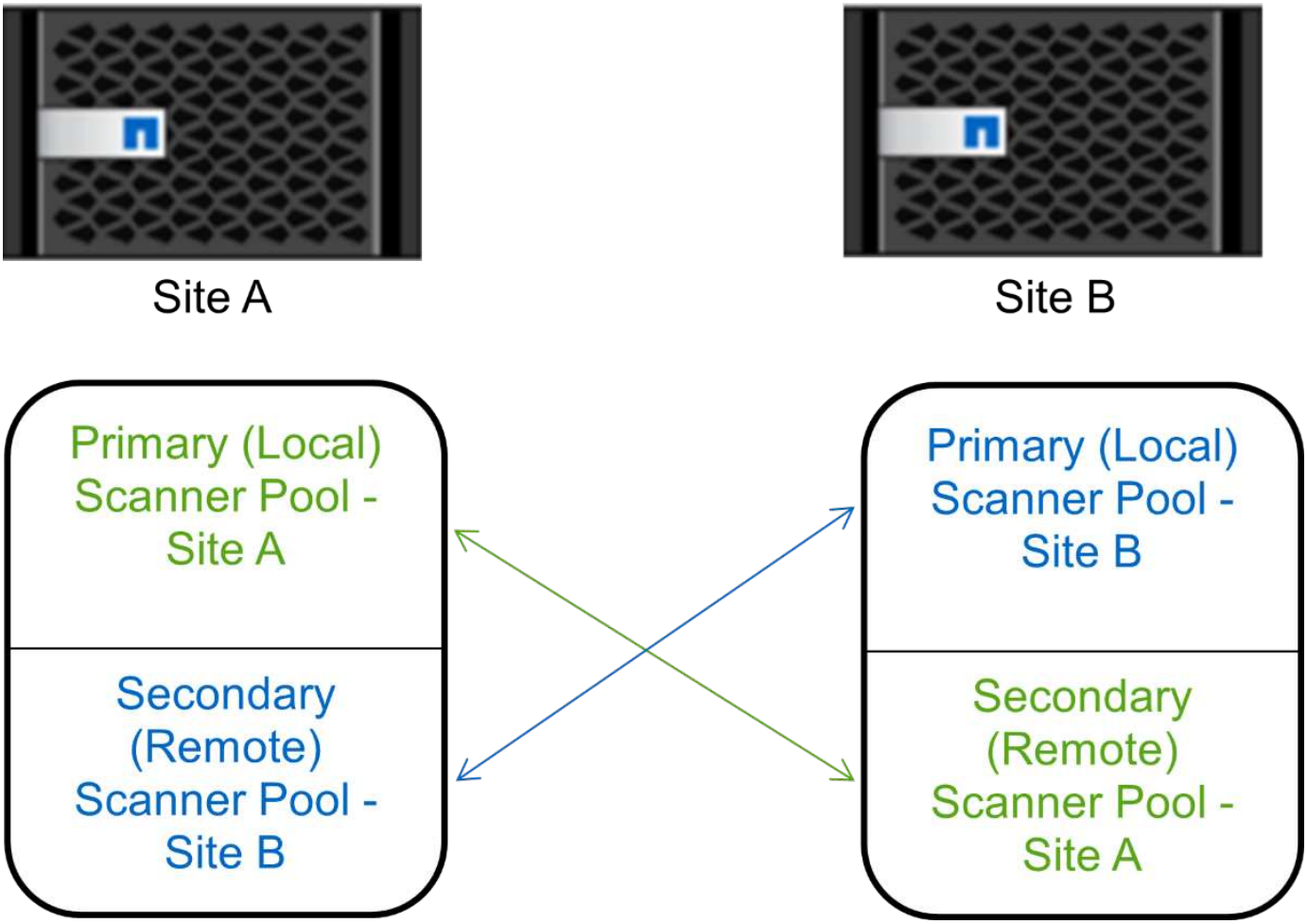
- A lista de usuários privilegiados deve incluir a conta de usuário do domínio que o servidor Vscan usa para se conetar ao SVM.
- Depois que o pool do scanner estiver configurado, verifique o status da conexão com os servidores.

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 com o ONTAP

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 `vserver vscan on-demand-task create` o "Referência do comando ONTAP"na .

  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

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
---------------------------------------------------------------
```

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

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 de 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 compatível com vários volumes, mas ainda não está configurada.
Os SVMs não estão configurados para proteção autônoma contra ransomware	A proteção autônoma contra ransomware é compatível com 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 limite combinado para SVMs habilitadas para auditoria NFS e S3 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.

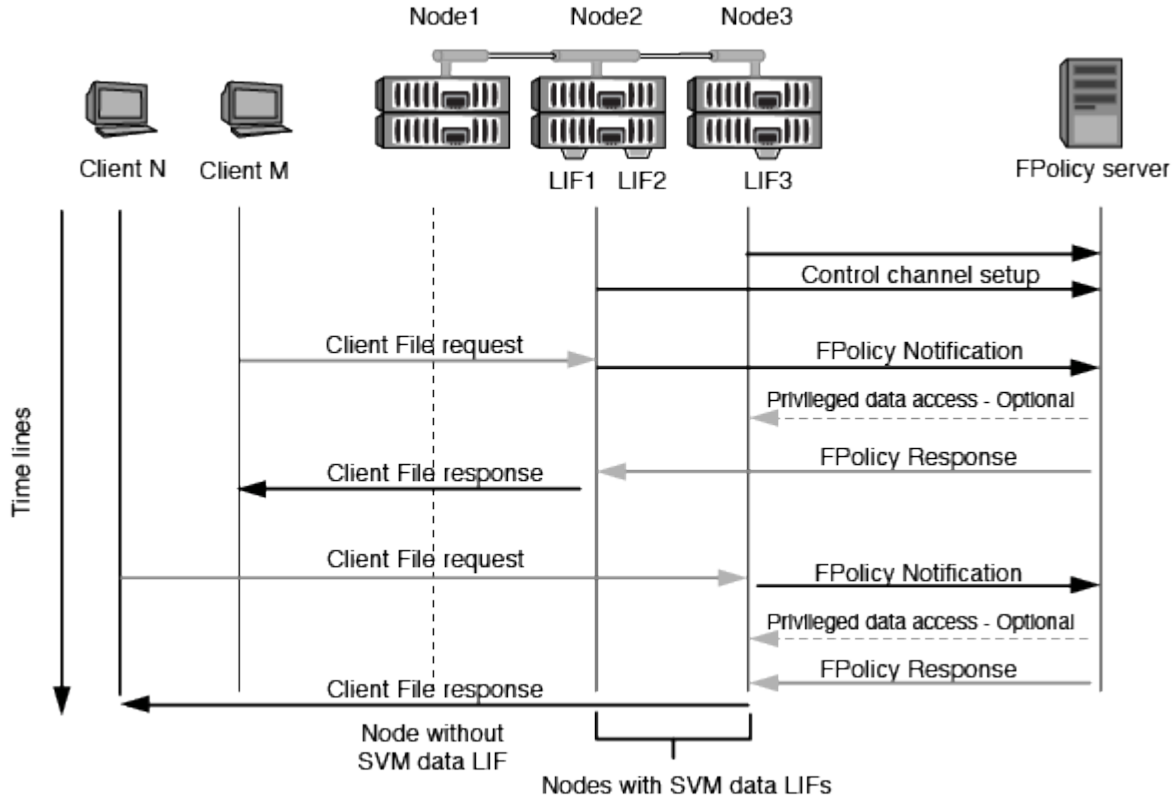
Cada nó que participa de cada máquina virtual de armazenamento (SVM) inicia uma conexão com um servidor FPolicy externo (servidor FPolicy) usando TCP/IP. As conexões com os servidores FPolicy são configuradas usando LIFs de dados de nó; portanto, um nó participante pode configurar uma conexão somente 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][`integer`s]

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. Não exclua 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.

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.

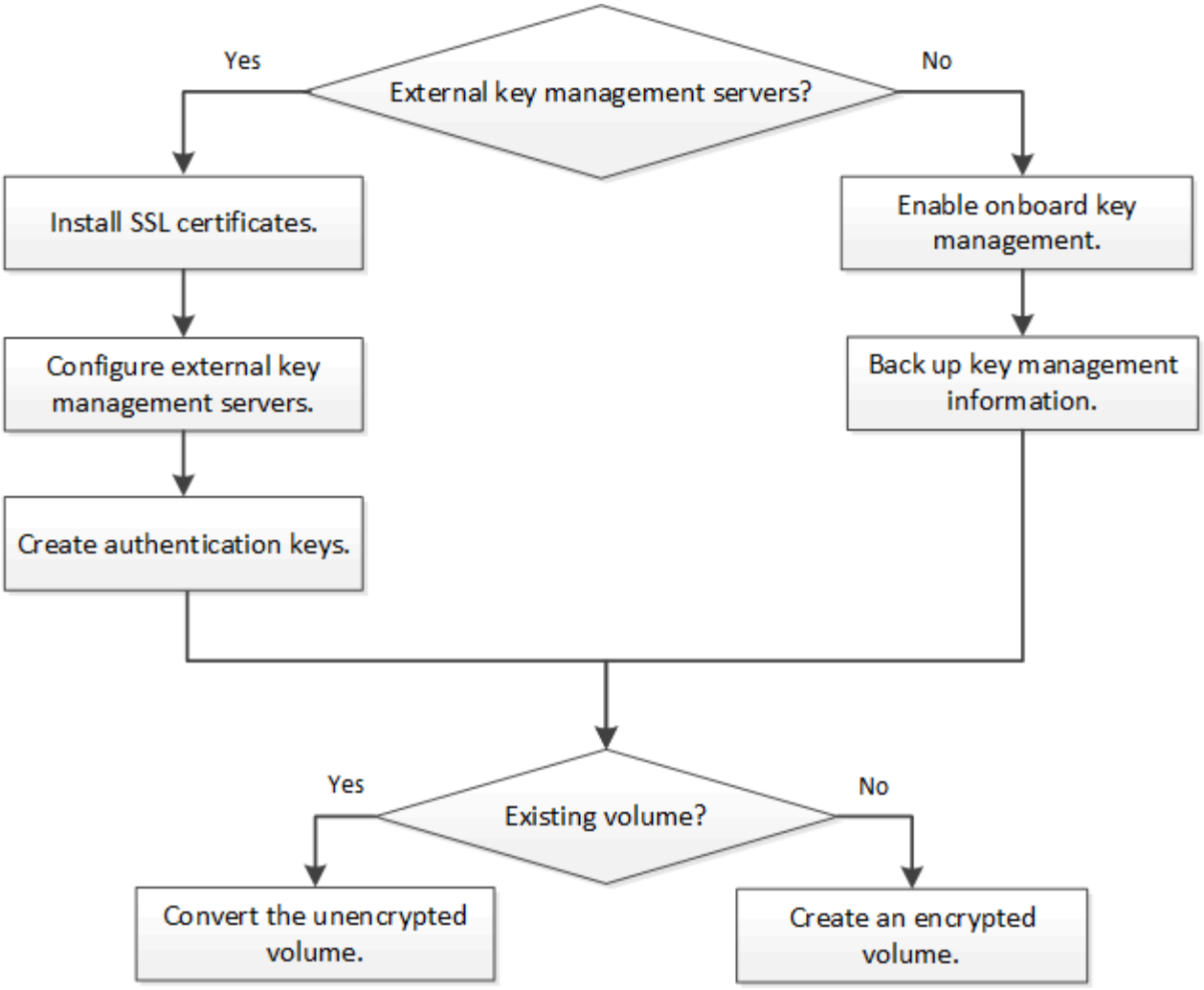
Replicação	• Para replicação de volume, os volumes de origem e destino podem ter configurações de criptografia diferentes. A criptografia pode ser configurada para a origem e não configurada para o destino e vice-versa. A encriptação configurada na origem não será replicada para o destino. A criptografia 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 `volume create` o "Referência do comando ONTAP"na .

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

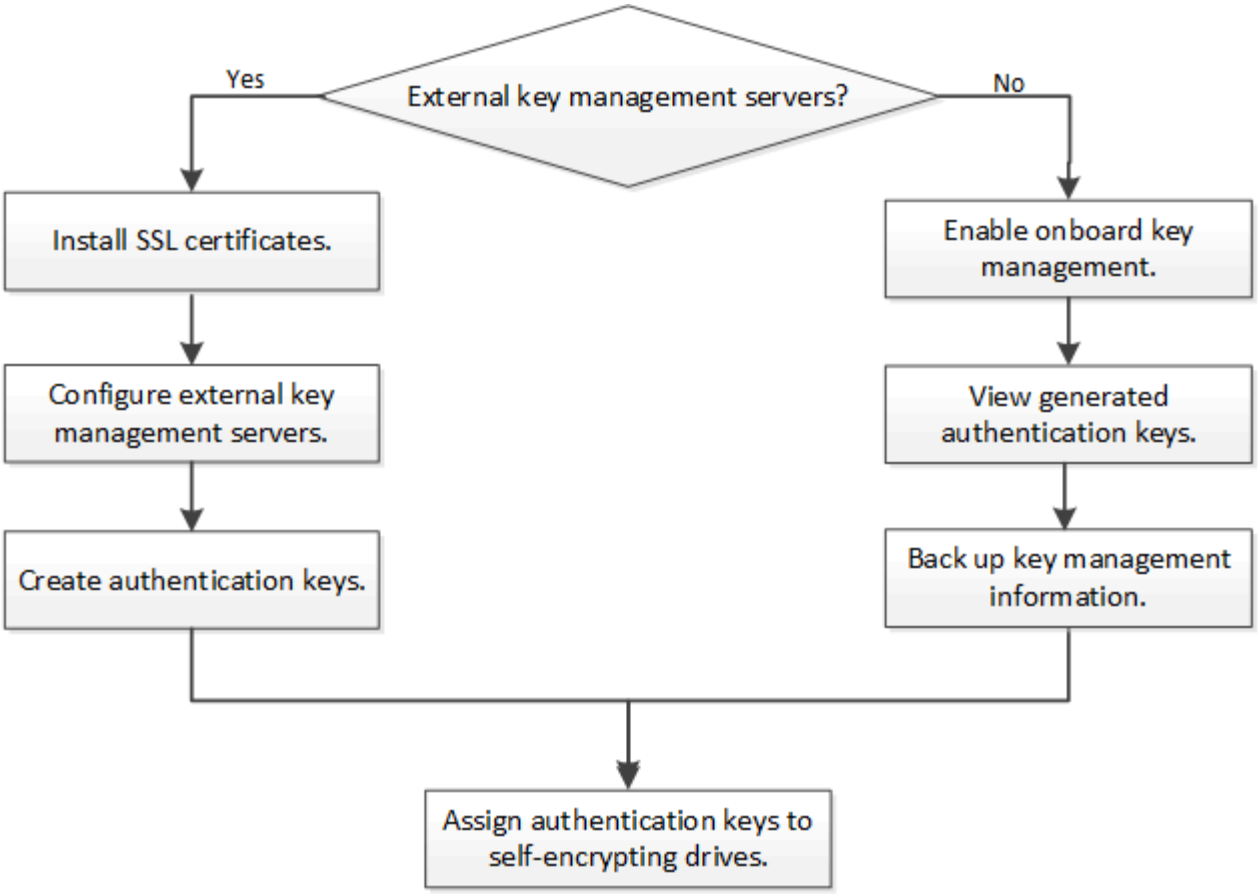
A tabela a seguir mostra detalhes importantes do suporte à criptografia de hardware. Consulte a Matriz de interoperabilidade para obter as informações mais recentes sobre servidores KMIP, sistemas de storage e compartimentos de disco compatíveis.

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--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAIgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAgAAAAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     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.

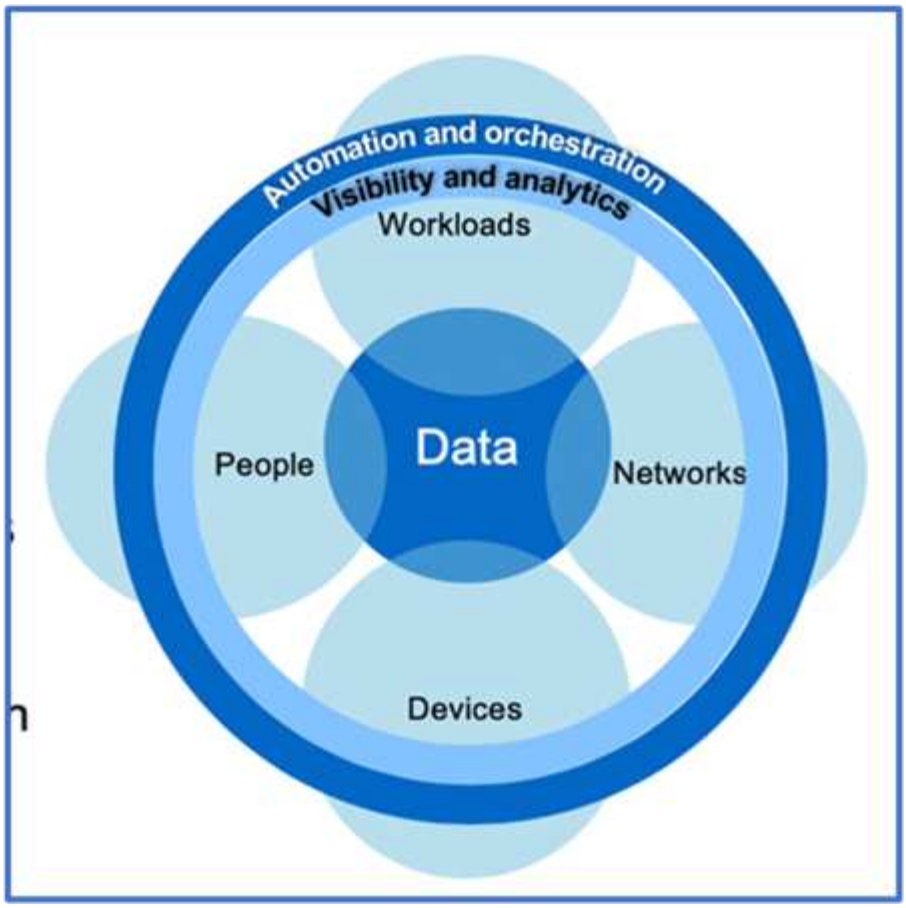
Recursos de segurança

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.

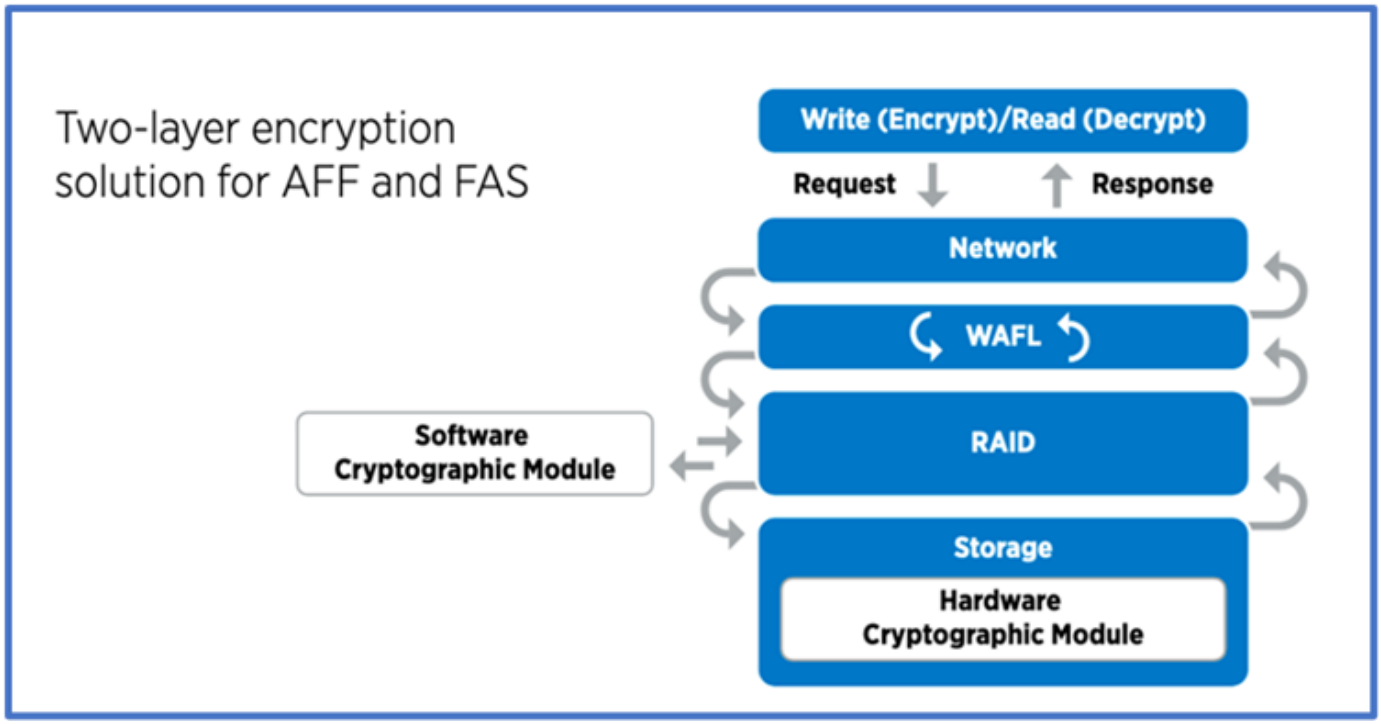
Uso de criptografia para dados em repouso e dados em trânsito

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.

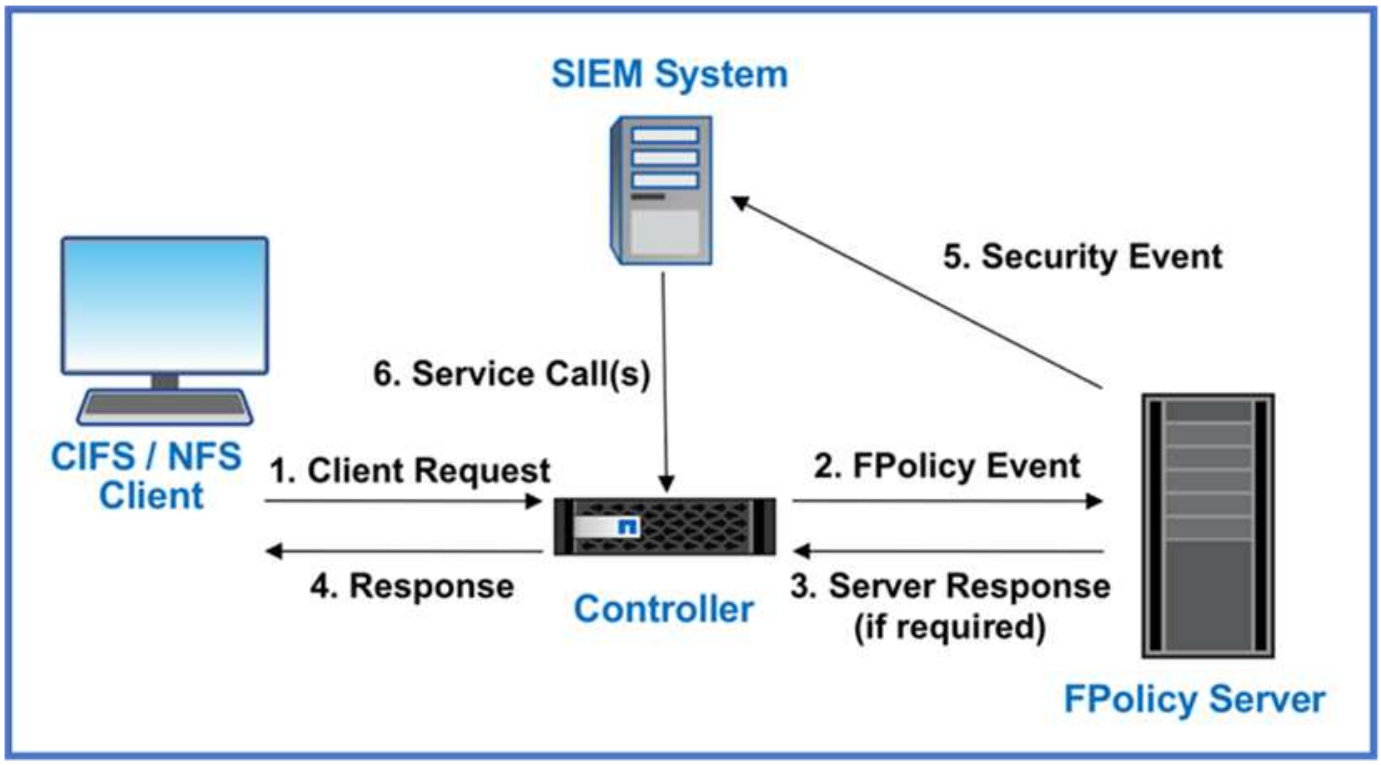
Criptografia de dados em trânsito

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais