Documentação do ASA r2

ASA r2

NetApp
February 11, 2026

Índice

Documentação do ASA r2

Notas de lançamento

Novidades no ONTAP 9.18.1 para sistemas ASA r2

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.18.1 para sistemas ASA r2.

Proteção de dados

Atualização	Descrição
"Suporte aprimorado para configurações de sincronização ativa do SnapMirror."	O suporte para sincronização ativa do SnapMirror foi ampliado de clusters de dois nós para clusters de quatro nós.

Rede

Atualização	Descrição
"Descarregamento de hardware IPsec Suporte a IPv6"	O suporte ao descarregamento de hardware IPsec foi estendido ao IPv6.
"Algoritmos OpenSSL PQC"	O ONTAP oferece suporte a algoritmos criptográficos de computação pós-quântica para SSL. Esses algoritmos fornecem proteção adicional contra possíveis ataques futuros de computação quântica e estão disponíveis quando o modo SSL FIPS está desativado.

Migração de dados SAN

Atualização	Descrição
"Suporte para migração de VMs de armazenamento"	Você pode migrar uma máquina virtual (VM) de armazenamento de um cluster ASA para um cluster ASA R2 sem interrupções. Isso permite que cargas de trabalho em bloco sejam migradas para sistemas ASA r2, preservando a integridade dos dados e garantindo que não haja impacto nos aplicativos. O processo de migração foi projetado para manter os mapeamentos de host e as configurações de LUN existentes, reduzindo o esforço operacional e o risco durante a migração.

Segurança

Atualização	Descrição
"Suporte para capacitação automática de ARP/AI"	Ao inicializar um novo cluster ASA r2 9.18.1 ou atualizar seu cluster para 9.18.1, o ARP/AI é ativado automaticamente por padrão em todas as unidades de armazenamento recém-criadas após um período de carência de 12 horas. Se você não desativar o ARP/AI durante o período de carência, ele será ativado em todo o cluster para as unidades de armazenamento recém-criadas quando o período de carência terminar.

Eficiência de storage

Atualização	Descrição
"Suporte para descarregamento de cópia NVMe"	O recurso de descarregamento de cópia NVMe permite que um host NVMe transfira as operações de cópia de sua CPU para a CPU do controlador de armazenamento ONTAP . O host pode copiar dados de um namespace NVMe para outro, reservando seus recursos de CPU para cargas de trabalho de aplicativos.
"Suporte para modificação da reserva de snapshots e exclusão automática de snapshots."	Você pode modificar a reserva de snapshots e ativar a exclusão automática de snapshots para limitar a quantidade de espaço usada para snapshots em suas unidades de armazenamento ASA r2. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Isso evita interrupções nos aplicativos, impedindo que os snapshots consumam espaço na sua unidade de armazenamento destinada aos dados do usuário.

Novidades no ONTAP 9.17.1 para sistemas ASA r2

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.17.1 para sistemas ASA r2.

Migração de dados SAN

Atualização	Descrição
"Suporte para migração de dados de um sistema de armazenamento de terceiros"	A migração de dados SAN usando Importação de LUN Estrangeiro (FLI) é compatível com sistemas ASA r2. A FLI permite migrar dados de um LUN em um sistema de armazenamento de terceiros para um sistema ASA r2.

Proteção de dados

Atualização	Descrição
"Suporte para proteção autônoma contra ransomware com inteligência artificial (ARP/IA)"	O ARP/AI pode ser habilitado em unidades de armazenamento ASA r2. O ARP/AI oferece proteção adicional de dados, detectando e reportando potenciais ataques de ransomware sem período de aprendizagem.
"Suporte SnapMirror Active Sync para protocolos NVMe"	O SnapMirror Active Sync adiciona suporte para cargas de trabalho VMware com acesso a hosts NVMe/TCP e NVMe/FC para clusters ONTAP de dois nós. O suporte a cargas de trabalho VMware para NVMe/TCP depende da resolução do bug da VMware ID: TR1049746.
"Suporte para alterações de geometria em grupos de consistência em relacionamentos de replicação"	Os sistemas ASA r2 oferecem suporte a alterações de geometria em grupos de consistência em uma sincronização ativa do SnapMirror ou em um relacionamento de replicação assíncrona sem excluir o relacionamento de sincronização ativa do SnapMirror ou interromper o relacionamento assíncrono. Quando ocorre uma alteração na geometria do grupo de consistência primário, a alteração é replicada para o grupo de consistência secundário.

Atualização	Descrição
"Suporte para replicação assíncrona de grupos de consistência filhos"	Políticas de replicação assíncrona podem ser aplicadas a grupos de consistência em relacionamentos hierárquicos.

Gerenciamento de storage

Atualização	Descrição
"Suporte para balanceamento automático de carga de trabalho"	As cargas de trabalho são balanceadas automaticamente entre os nós de um par de HA para otimizar o desempenho e a utilização de recursos.

Novidades do ONTAP 9.16,1 para sistemas ASA R2

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.16,1 para sistemas ASA R2.

Sistemas

Atualização	Descrição
Sistemas	Os seguintes sistemas NetApp ASA r2 são suportados a partir do ONTAP 9.16.1. Esses sistemas oferecem uma solução unificada de hardware e software que cria uma experiência simplificada, específica para as necessidades de clientes que utilizam apenas SAN. • ASA A50 • ASA A30 • ASA A20 • ASA C30

Proteção de dados

Atualização	Descrição
"Suporte para migração de chave de criptografia entre gerenciadores de chaves"	Ao alternar do gerenciador de chaves integrado do ONTAP para um gerenciador de chaves externo no nível do cluster, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar facilmente as chaves de criptografia de um gerenciador de chaves para o outro.
"Suporte para grupos hierárquicos de consistência"	Os grupos hierárquicos de consistência permitem criar um grupo de consistência pai que contém vários grupos filhos de consistência. Isso simplifica a proteção e o gerenciamento de dados para estruturas de dados complexas.

Suporte ao protocolo

Atualização	Descrição
"Suporte a NVMe para multipathing ativo-ativo simétrico"	O NVMe/FC e o NVMe/TCP agora oferecem suporte à arquitetura ativo-ativo simétrica para multipathing de modo que todos os caminhos entre os hosts e o storage estejam ativos/otimizados.

Eficiência de storage

Atualização	Descrição
"Suporte para rebalanceamento automático de unidades de armazenamento"	O ONTAP reequilibrará automaticamente as unidades de storage nas zonas de disponibilidade de storage para obter performance e utilização de capacidade ideais.
"Alocação de espaço NVMe habilitada por padrão"	A alocação de espaço (também chamada de "perfuração" e "desmapear") é habilitada para namespaces NVMe por padrão. A desalocação de espaço permite que um host inutilize blocos de nomes para recuperar espaço. Isso melhora muito a eficiência geral do storage, especialmente com sistemas de arquivos que têm alta rotatividade de dados.

Novidades do ONTAP 9.16,0 para sistemas ASA R2

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.16,0 para sistemas ASA R2.

Sistemas

Atualização	Descrição
Sistemas	Os seguintes sistemas NetApp ASA r2 estão disponíveis. Esses sistemas oferecem uma solução unificada de hardware e software que cria uma experiência simplificada, específica para as necessidades de clientes que utilizam apenas SAN. • ASA A1K • ASA A70 • ASA A90

System Manager

Atualização	Descrição
"Suporte otimizado para clientes somente de SAN"	O System Manager é otimizado para oferecer suporte à funcionalidade essencial de SAN, ao mesmo tempo em que remove a visibilidade de recursos e funções não compatíveis em ambientes SAN.

Gerenciamento de storage

Atualização	Descrição
"Gerenciamento simplificado de storage"	Os sistemas ASA R2 apresentam o uso de unidades de storage com grupos de consistência para gerenciamento simplificado de storage. • Uma *unidade de armazenamento* torna o espaço de armazenamento disponível para seus hosts SAN para operações de dados. Uma unidade de storage refere-se a um LUN para hosts SCSI ou a um namespace NVMe para hosts NVMe. • *Um grupo de consistência* é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade.

Segurança dos dados

Atualização	Descrição
"Gerenciador de chaves integrado e criptografia de camada dupla"	Os sistemas ASA R2 são compatíveis com um gerenciador de chaves integrado e criptografia de camada dupla (hardware e software).

Alterações nos limites e padrões do ONTAP que afetam os sistemas ASA R2

Saiba mais sobre as alterações nos limites e padrões que afetam os sistemas ASA R2. A NetApp se esforça para ajudar seus clientes a entender os padrões mais importantes e limitar as alterações em cada versão do ONTAP.

Alterações nos limites do ONTAP

Recurso	Limite de alteração	Alterado na versão…
VMs de armazenamento por cluster	O número máximo de máquinas virtuais (VMs) de armazenamento suportadas por par HA foi aumentado de 32 para 256.	ONTAP 9.18.1
SnapMirror sincronização ativa	O suporte para SnapMirror active sync foi ampliado de clusters de dois nós para clusters de quatro nós.	ONTAP 9.18.1
Nós por cluster	O número máximo de nós por cluster aumenta de 2 para 12. Se você estiver executando o ONTAP 9.16.1 com mais de 2 nós em um cluster, não será possível reverter para o ONTAP 9.16.0.	ONTAP 9.16,1

Recurso	Limite de alteração	Alterado na versão…
Unidades de armazenamento	O número máximo de unidades de storage é aumentado de 2500 por par de HA para 10.000 por par de HA.	ONTAP 9.16,1

Comece agora

Saiba mais sobre os sistemas de armazenamento ASA R2

Os sistemas NetApp ASA R2 fornecem uma solução unificada de hardware e software que cria uma experiência simplificada específica para as necessidades dos clientes somente de SAN.

Os seguintes sistemas são classificados como sistemas ASA r2:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Os sistemas ASA r2 suportam todos os protocolos SAN (iSCSI, FC, NVMe/FC, NVMe/TCP). Os protocolos iSCSI, FC, NVMe/FC e NVMe/TCP oferecem suporte à arquitetura simétrica ativa-ativa para multicaminhos, de modo que todos os caminhos entre os hosts e o armazenamento sejam ativos/otimizados. Os protocolos iSCSI e NVMe/TCP suportam conexão direta entre os hosts e o armazenamento. Para os protocolos Fibre Channel e NVMe/FC, a conexão direta não é suportada.

Em um sistema ASA R2, o software ONTAP e o Gerenciador de sistemas são otimizados para oferecer suporte à funcionalidade essencial de SAN, removendo recursos e funções não compatíveis em ambientes SAN.

Os sistemas ASA R2 introduzem o uso de unidades de storage com grupos de consistência:

- Uma *unidade de armazenamento* torna o espaço de armazenamento disponível para seus hosts SAN para operações de dados. Uma unidade de storage refere-se a um LUN para hosts SCSI ou a um namespace NVMe para hosts NVMe.
- *Um grupo de consistência* é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade.

Os sistemas ASA r2 usam unidades de armazenamento com grupos de consistência para simplificar o gerenciamento de armazenamento e a proteção de dados. Por exemplo, suponha que você tenha um banco de dados com 10 unidades de armazenamento em um grupo de consistência e precise fazer backup de todo o banco de dados. Em vez de fazer backup de cada unidade de armazenamento individualmente, você pode proteger todo o banco de dados fazendo backup do grupo de consistência.

Para ajudar a proteger seus dados contra ataques maliciosos, como roubo ou ransomware, os sistemas ASA r2 oferecem suporte a um gerenciador de chaves integrado, criptografia de camada dupla, autenticação multifator e verificação multiadministradora. Snapshots à prova de violação também são suportados em sistemas ASA r2 secundários.

Os sistemas ASA r2 não oferecem suporte à mistura de clusters com sistemas ASA, AFF ou FAS .

Para mais informações

- Saiba mais sobre o suporte e as limitações dos sistemas ASA R2 no "NetApp Hardware Universe".
- Saiba mais "Os sistemas ASA R2 em comparação com os sistemas ASA"sobre o .
- Saiba mais sobre o "NetApp ASA".

Início rápido para sistemas de storage ASA R2

Para começar a funcionar com o sistema ASA R2, instale os componentes de hardware, configure o cluster, configure o acesso aos dados dos hosts para o sistema de storage e provisione o storage.

Instale e configure o hardware

"Instale e configure" Seu sistema ASA R2 e implantá-lo em seu ambiente ONTAP.

Configure o cluster

Use o System Manager para guiá-lo através de um processo rápido e fácil para "Configure o cluster do ONTAP".

Configure o acesso aos dados

"Conete seu sistema ASA R2 aos seus clientes SAN".

Provisione seu storage

"Provisionamento de storage" Para começar a fornecer dados aos seus clientes SAN.

O que se segue?

Agora você pode usar o System Manager para proteger seus dados pelo "criar instantâneos".

Instale o sistema ASA R2

Fluxo de trabalho de instalação e configuração para sistemas de storage ASA R2

Para instalar e configurar o sistema ASA r2, você analisa os requisitos de hardware, prepara o site, instala e faz o cabo dos componentes de hardware, liga o sistema e configura o cluster do ONTAP.

"Revise os requisitos de instalação de hardware"

Verifique os requisitos de hardware para instalar o sistema de storage ASA R2.

"Prepare-se para instalar o sistema de storage ASA r2"

Para se preparar para instalar o sistema ASA R2, você precisa preparar o local, verificar os requisitos

ambientais e elétricos e garantir que há espaço suficiente no rack. Em seguida, desembale o equipamento, compare seu conteúdo com o deslizamento de embalagem e Registre o hardware para acessar os benefícios de suporte.

3 **"Instale o hardware do sistema de storage ASA r2"**

Para instalar o hardware, instale os kits de trilho para o seu sistema de armazenamento e prateleiras e, em seguida, instale e proteja o sistema de armazenamento no gabinete ou rack de telecomunicações. Em seguida, deslize as prateleiras sobre os trilhos. Finalmente, conete dispositivos de gerenciamento de cabos à parte traseira do sistema de armazenamento para roteamento organizado de cabos.

4 **"Faça o cabeamento das controladoras e gavetas de storage do sistema de storage ASA r2"**

Para fazer o cabeamento do hardware, primeiro conete os controladores de storage à rede e, em seguida, conete os controladores às gavetas de storage.

5 **"Ligue o sistema de armazenamento ASA r2"**

Antes de ligar os controladores, ligue cada gaveta NS224 e atribua um ID exclusivo do compartimento para garantir que cada gaveta seja identificada exclusivamente na configuração.

Requisitos de instalação para sistemas de storage ASA R2

Reveja o equipamento necessário e as precauções de elevação para o seu sistema de armazenamento ASA r2 e prateleiras de armazenamento.

Equipamento necessário para instalação

Para instalar o sistema de storage ASA r2, você precisa dos seguintes equipamentos e ferramentas.

- Acesso a um navegador da Web para configurar o sistema de armazenamento
- Fita de descarga eletrostática (ESD)
- Lanterna
- Computador portátil ou console com conexão USB/serial
- Clipe de papel ou caneta esferográfica de ponta estreita para definir IDs de prateleira de armazenamento
- Chave de fendas Phillips nº 2

Precauções de elevação

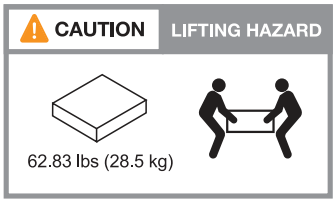
Os sistemas de storage e as gavetas de storage do ASA R2 são pesados. Tenha cuidado ao levantar e mover estes itens.

Pesos do sistema de armazenamento

Tome as precauções necessárias ao mover ou elevar o seu sistema de armazenamento ASA R2.

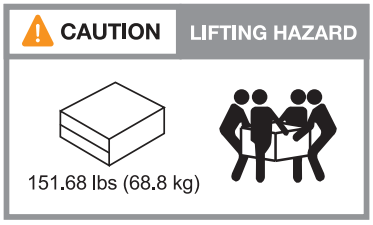
A1K

Um sistema de armazenamento ASA A1K pode pesar até 28,5 kg (62,83 lbs). Para levantar o sistema de armazenamento, utilize duas pessoas ou um elevador hidráulico.



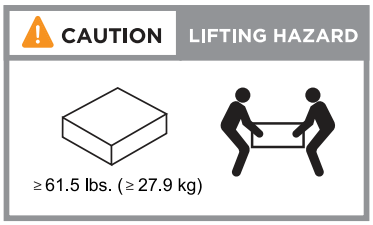
A70 e A90

Um sistema de armazenamento ASA A70 ou ASA A90 pode pesar até 151,68 lbs (68,8 kg). Para levantar o sistema de armazenamento, utilize quatro pessoas ou um elevador hidráulico.



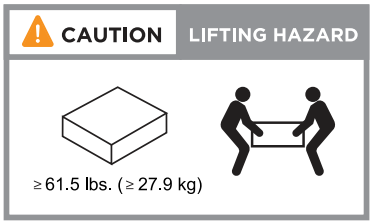
A20, A30 E A50

Um sistema de armazenamento ASA A20, ASA A30 ou ASA A50 pode pesar até 27,9 kg (61,5 lbs). Para levantar o sistema de armazenamento, utilize duas pessoas ou um elevador hidráulico.



C30

Um sistema de armazenamento ASA C30 pode pesar até 27,9 kg (61,5 lbs). Para levantar o sistema de armazenamento, utilize duas pessoas ou um elevador hidráulico.

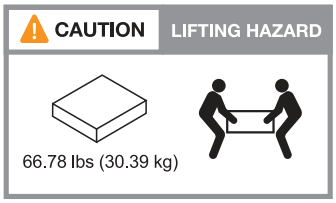


Pesos da prateleira de armazenamento

Tome as precauções necessárias ao mover ou levantar a prateleira.

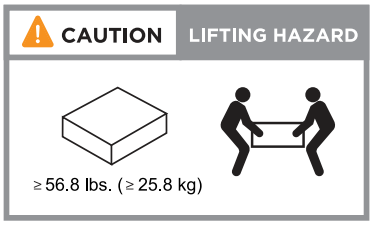
NS224 gaveta

Uma prateleira de NS224 kg pode pesar até 66,78 lbs (30,29 kg). Para levantar a prateleira, use duas pessoas ou um elevador hidráulico. Mantenha todos os componentes na prateleira (dianteira e traseira) para evitar desequilibrar o peso da prateleira.



NS224 gaveta com NSM100B módulos

Uma prateleira NS224 com NSM100B módulos pode pesar até 56,8 lbs (25,8 kg). Para levantar a prateleira, use duas pessoas ou um elevador hidráulico. Mantenha todos os componentes na prateleira (dianteira e traseira) para evitar desequilibrar o peso da prateleira.



Informações relacionadas

- "Informações de segurança e avisos regulamentares"

O que se segue?

Depois de analisar os requisitos de hardware, você "Prepare-se para instalar o sistema de storage ASA r2".

Prepare-se para instalar um sistema de storage ASA R2

Prepare-se para instalar seu sistema de armazenamento ASA r2, preparando o site, desembalando as caixas e comparando o conteúdo das caixas com o slip de embalagem e registrando o sistema para acessar os benefícios de suporte.

Passo 1: Prepare o site

Para instalar o sistema de armazenamento ASA R2, certifique-se de que o local e o gabinete ou rack que você planeja usar atendam às especificações de sua configuração.

Passos

1. Use "NetApp Hardware Universe" para confirmar se o local atende aos requisitos ambientais e elétricos do sistema de armazenamento.
2. Certifique-se de ter espaço adequado para o gabinete ou rack para o seu sistema de armazenamento, prateleiras e todos os switches:

A1K

- 4U em uma configuração de HA
- 2U TB para cada compartimento de armazenamento de NS224 TB
- 1U para a maioria dos interrutores

A70 e A90

- 4U em uma configuração de HA
- 2U TB para cada compartimento de armazenamento de NS224 TB
- 1U para a maioria dos interrutores

A20, A30 E A50

- 2U para um sistema de storage
- 2U TB para cada compartimento de armazenamento de NS224 TB
- 1U para a maioria dos interrutores

C30

- 2U para um sistema de storage
- 2U TB para cada compartimento de armazenamento de NS224 TB
- 1U para a maioria dos interrutores

3. Instale todos os switches de rede necessários.

   Consulte o "Documentação do switch" para obter instruções de instalação e "NetApp Hardware Universe" para obter informações sobre compatibilidade.

Passo 2: Desembale as caixas

Depois de garantir que o local e o gabinete ou rack que você planeja usar para o seu sistema de armazenamento ASA R2 atendam às especificações necessárias, desembale todas as caixas e compare o conteúdo com os itens no folheto de embalagem.

Passos

1. Abra cuidadosamente todas as caixas e coloque o conteúdo de forma organizada.
2. Compare o conteúdo que você descompactou com a lista no folheto de embalagem. Se houver discrepâncias, anote-as para outras ações.

   Você pode obter sua lista de embalagem digitalizando o código QR no lado da caixa de transporte.

   Os itens a seguir são alguns dos conteúdos que você pode ver nas caixas.

Hardware	Cabos	

• Painel frontal • Sistema de storage • Kits de trilhos com instruções (opcional) • Prateleira de armazenamento (se você pediu armazenamento adicional)	• Cabos Ethernet de gerenciamento (cabos RJ-45) • Cabos de rede • Cabos de energia • Cabos de armazenamento (se você tiver pedido armazenamento adicional) • Cabo de porta serial USB-C.	

Passo 3: Registre seu sistema de armazenamento

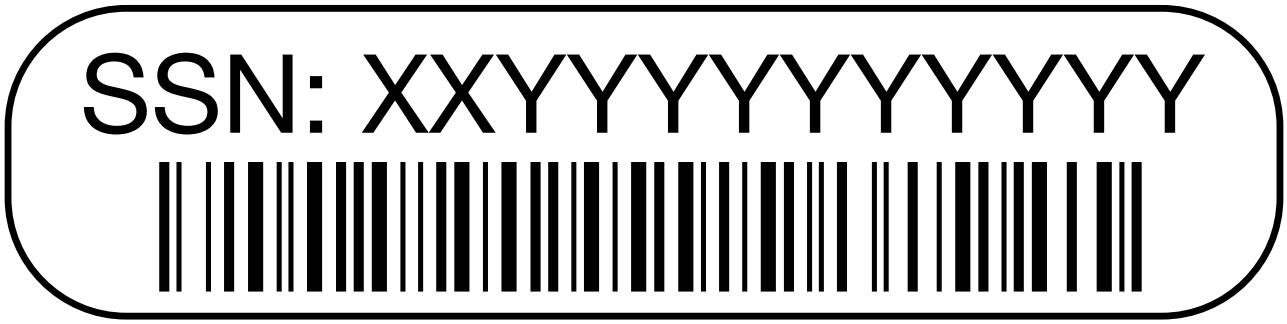
Depois de garantir que seu local atenda aos requisitos das especificações do sistema de storage ASA R2 e verificar se tem todas as peças que você solicitou, você deve Registrar seu sistema.

Passos

1. Localize os números de série do seu sistema de armazenamento.

   Você pode encontrar os números de série nos seguintes locais:

   - Sobre o deslizamento da embalagem
   - No seu e-mail de confirmação
   - Em cada controlador ou em alguns sistemas, no módulo de gestão do sistema de cada controlador



2. Vá para "Site de suporte da NetApp" .
3. Determine se você precisa Registrar seu sistema de storage:

Se você é um…	Siga estes passos…
Cliente NetApp existente	a. Inicie sessão com o seu nome de utilizador e palavra-passe. b. Selecione **sistemas** > **Meus sistemas**. c. Confirme se o novo número de série está listado. d. Se o número de série não estiver listado, siga as instruções para novos clientes NetApp.

Se você é um…	Siga estes passos…
Novo cliente da NetApp	a. Clique em **Registe-se agora** e crie uma conta. b. Selecione **Systems** > **Register Systems**. c. Introduza o número de série do sistema de armazenamento e os detalhes solicitados. Após a aprovação do seu registo, pode transferir qualquer software necessário. O processo de aprovação pode demorar até 24 horas.

O que se segue?

Depois de se preparar para instalar o hardware do ASA R2, "Instale o hardware do seu sistema de storage ASA r2"você .

Instale o sistema de storage ASA R2

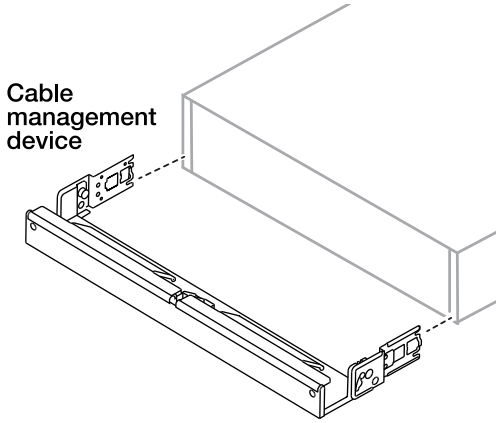
Depois de se preparar para instalar o sistema de storage ASA r2, instale o hardware do sistema. Primeiro, instale os kits de trilho. Em seguida, instale e proteja seu sistema de armazenamento em um gabinete ou rack de telecomunicações.

Antes de começar

- Certifique-se de que tem as instruções fornecidas com o kit de calha.
- Tenha em atenção os problemas de segurança associados ao peso do sistema de armazenamento e da prateleira de armazenamento.
- Entenda que o fluxo de ar através do sistema de armazenamento entra pela frente onde a tampa frontal ou as tampas da extremidade estão instaladas e esgota a parte traseira onde as portas estão localizadas.

Passos

1. Instale os kits de trilho para o seu sistema de armazenamento e prateleiras de armazenamento, conforme necessário, usando as instruções incluídas nos kits.
2. Instale e proteja seu sistema de armazenamento no gabinete ou rack de telecomunicações:
   a. Posicione o sistema de armazenamento nos trilhos no meio do gabinete ou rack de telecomunicações e, em seguida, apoie o sistema de armazenamento a partir da parte inferior e deslize-o para o lugar.
   b. Certifique-se de que os pinos-guia no gabinete ou no rack de telecomunicações se encaixem com segurança nos slots-guia do sistema de armazenamento.
   c. Fixe o sistema de armazenamento ao gabinete ou rack de telecomunicações usando os parafusos de montagem incluídos.
3. Fixe o painel frontal à parte frontal do sistema de armazenamento.
4. Se o seu sistema ASA R2 veio com um dispositivo de gerenciamento de cabos, conete-o à parte traseira do sistema de armazenamento.



5. Instale e fixe a prateleira de armazenamento:
   a. Posicione a parte de trás da prateleira de armazenamento sobre os trilhos e, em seguida, apoie a prateleira a partir da parte inferior e deslize-a para o gabinete ou rack de telecomunicações.

      Se você estiver instalando várias gavetas de storage, coloque o primeiro compartimento de storage diretamente acima das controladoras. Coloque o segundo compartimento de storage diretamente sob as controladoras. Repita este padrão para quaisquer prateleiras de armazenamento adicionais.

   b. Fixe a prateleira de armazenamento no gabinete ou rack de telecomunicações usando os parafusos de montagem incluídos.

O que se segue?

Depois de instalar o hardware para o sistema ASA R2, "Faça o cabeamento dos controladores e gavetas de storage do seu sistema ASA R2"você .

Cable o hardware do seu sistema de storage ASA R2

Depois de instalar o hardware de rack para seu sistema de storage ASA r2, instale os cabos de rede das controladoras e conete os cabos entre as controladoras e as gavetas de storage.

Antes de começar

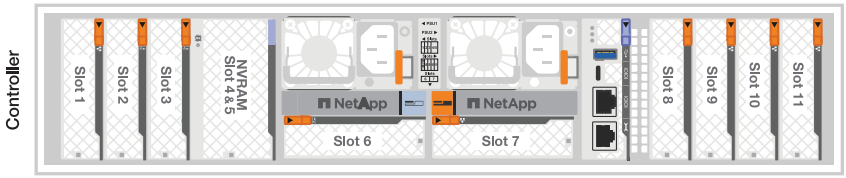
Contacte o administrador da rede para obter informações sobre como ligar o sistema de armazenamento aos comutadores de rede.

Sobre esta tarefa

- Esses procedimentos mostram configurações comuns. O cabeamento específico depende dos componentes solicitados para o seu sistema de storage. Para obter detalhes abrangentes de configuração e prioridade de slot, "NetApp Hardware Universe"consulte .
- Os procedimentos de cabeamento de rede de cluster/HA e host mostram configurações comuns.

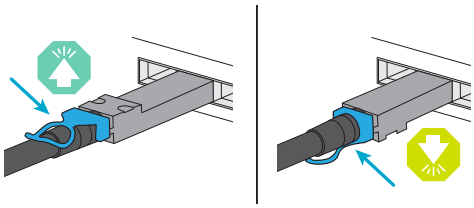
  Se você não vir sua configuração nos procedimentos de cabeamento, vá para "NetApp Hardware Universe" para obter informações abrangentes sobre configuração e prioridade de slots para cabear corretamente seu sistema de armazenamento.

- Se você tiver um sistema de armazenamento ASA A1K, ASA A70 ou ASA A90, os slots de E/S serão numerados de 1 a 11.



- Os gráficos de cabeamento têm ícones de seta mostrando a orientação adequada (para cima ou para baixo) da aba de puxar do conetor do cabo ao inserir um conetor em uma porta.

  Ao inserir o conetor, você deve sentir que ele clique no lugar; se você não sentir que ele clique, remova-o, vire-o e tente novamente.



- Se o cabeamento de um switch ótico for feito, insira o transcetor ótico na porta da controladora antes de fazer o cabeamento da porta do switch.

Etapa 1: Faça o cabeamento das conexões cluster/HA

Faça o cabeamento dos controladores ao cluster do ONTAP. Este procedimento difere dependendo do modelo do sistema de armazenamento e da configuração do módulo de e/S.

O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas.

A1K

Crie as conexões do cluster do ONTAP. Para clusters sem switch, conecte as controladoras umas às outras. Para clusters comutados, conete os controladores aos switches de rede do cluster.

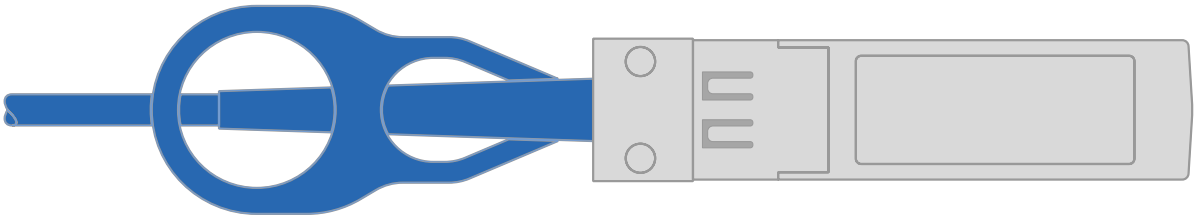
Cabeamento de cluster sem switch

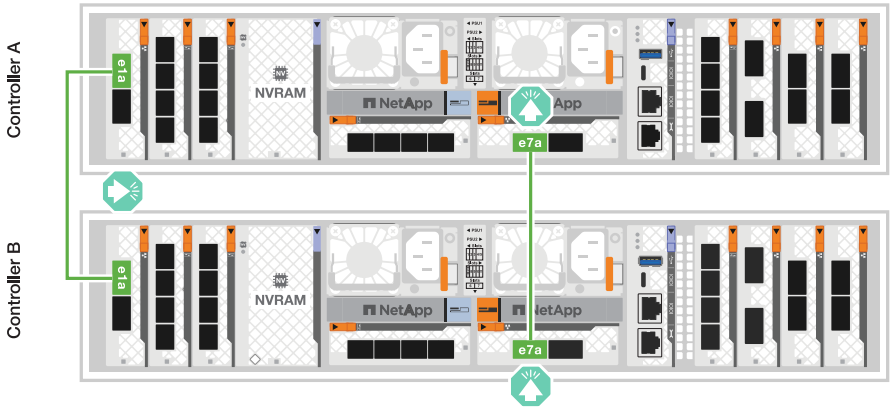
Use o cabo de interconexão cluster/HA para conetar as portas e1a a e1a e as portas e7a a e7a.

Passos

1. Conete a porta e1a no controlador A à porta e1a no controlador B.
2. Conete a porta e7a no controlador A à porta e1a no controlador B.

Cabos de interconexão de cluster/HA





Cabeamento de cluster comutado

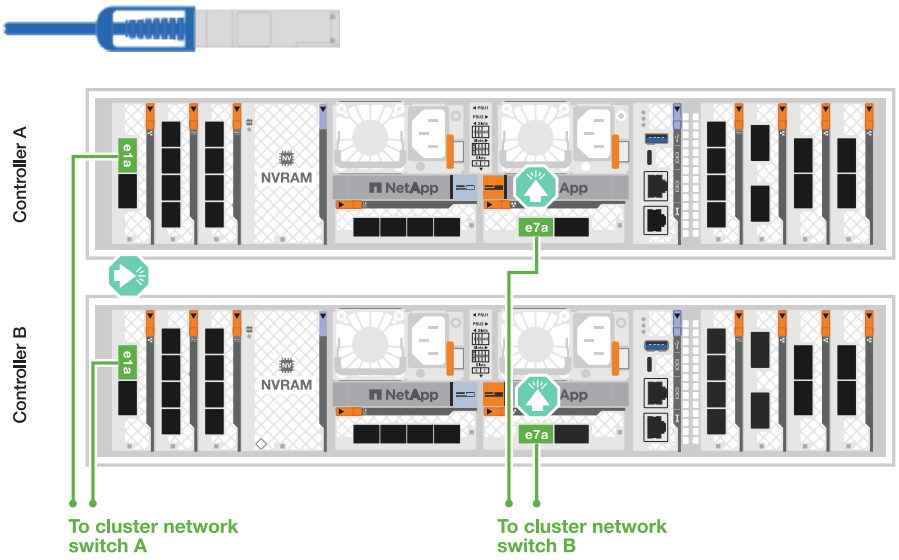
Use o cabo de 100 GbE para conetar as portas e1a a e1a e as portas e7a a e7a.

As configurações de cluster comutado são suportadas no 9.16.1 e versões posteriores.

Passos

1. Conete a porta e1a no controlador A e a porta e1a no controlador B ao switch de rede do cluster A..
2. Conete a porta e7a no controlador A e a porta e7a no controlador B ao switch de rede do cluster B.

Cabo de 100 GbE



A70 e A90

Crie as conexões do cluster do ONTAP. Para clusters sem switch, conecte as controladoras umas às outras. Para clusters comutados, conete os controladores aos switches de rede do cluster.

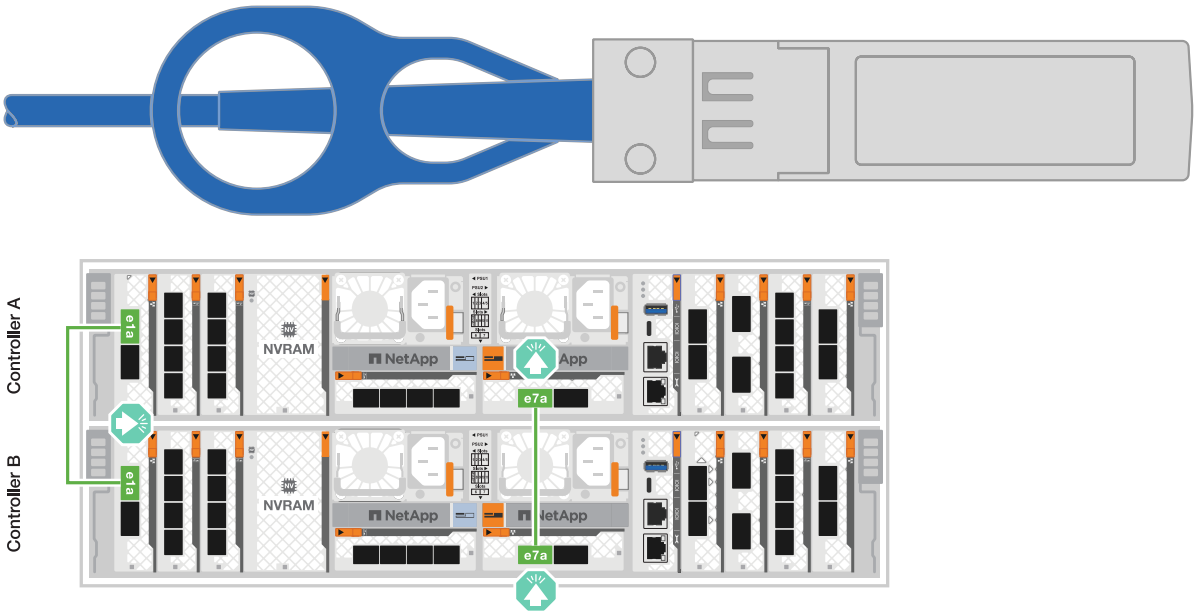
Cabeamento de cluster sem switch

Use o cabo de interconexão cluster/HA para conetar as portas e1a a e1a e as portas e7a a e7a.

Passos

1. Conete a porta e1a no controlador A à porta e1a no controlador B.
2. Conete a porta e7a no controlador A à porta e1a no controlador B.

Cabos de interconexão de cluster/HA



Cabeamento de cluster comutado

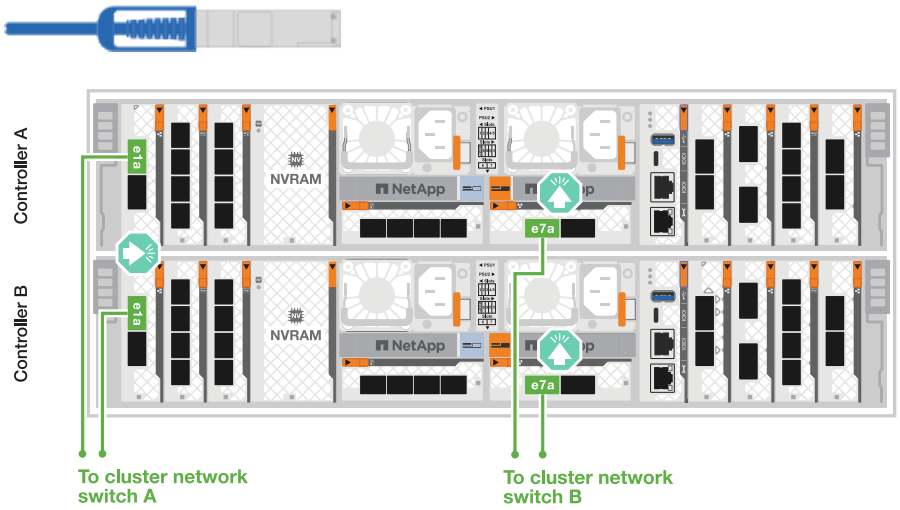
Use o cabo de 100 GbE para conetar as portas e1a a e1a e as portas e7a a e7a.

As configurações de cluster comutado são suportadas no 9.16.1 e versões posteriores.

Passos

1. Conete a porta e1a no controlador A e a porta e1a no controlador B ao switch de rede do cluster A..
2. Conete a porta e7a no controlador A e a porta e7a no controlador B ao switch de rede do cluster B.

Cabo de 100 GbE



A20, A30 E A50

Crie as conexões do cluster do ONTAP. Para clusters sem switch, conecte as controladoras umas às outras. Para clusters comutados, conete os controladores aos switches de rede do cluster.

Os exemplos de cabeamento de cluster/HA mostram configurações comuns.

Se você não vê sua configuração aqui, vá para "NetApp Hardware Universe" para obter informações abrangentes sobre configuração e prioridade de slots para cabear seu sistema de armazenamento.

Cabeamento de cluster sem switch

Conete os controladores uns aos outros para criar as conexões do cluster do ONTAP.

ASA A30 e ASA A50 com dois módulos de e/S de 40/100 GbE de 2 portas

Passos

1. Conete as conexões de interconexão cluster/HA:

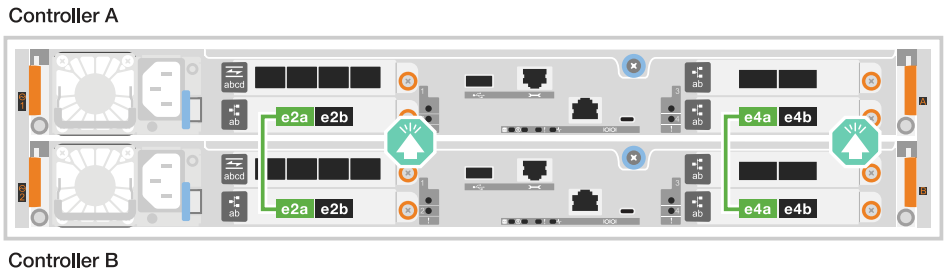
   O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (nos módulos de e/S nos slots 2 e 4). As portas são de 40/100 GbE.

   a. Conete a porta E2A do controlador A à porta E2A do controlador B.

   b. Conete a porta e4a do controlador A à porta e4a do controlador B.

   As portas E2B e e4b do módulo de e/S não são utilizadas e estão disponíveis para conetividade de rede de host.

Cabos de interconexão de cluster/HA de 100 GbE



ASA A30 e ASA A50 com um módulo de e/S de 40/100 GbE de 2 portas

Passos

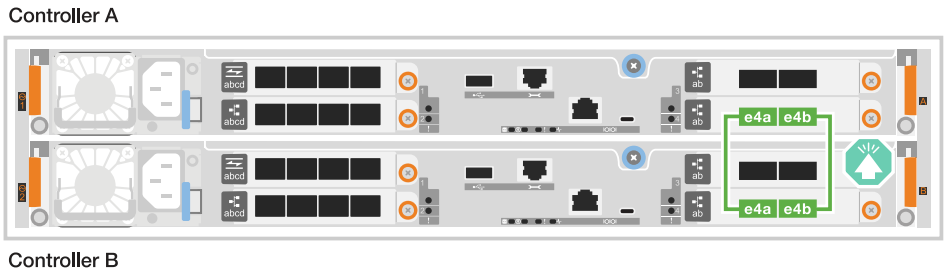
1. Conete as conexões de interconexão cluster/HA:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 40/100 GbE.

a. Conete a porta e4a do controlador A à porta e4a do controlador B.

b. Conete a porta e4b do controlador A à porta e4b do controlador B.

Cabos de interconexão de cluster/HA de 100 GbE



ASA A20 com um módulo de e/S de 10/25 GbE de 2 portas

Passos

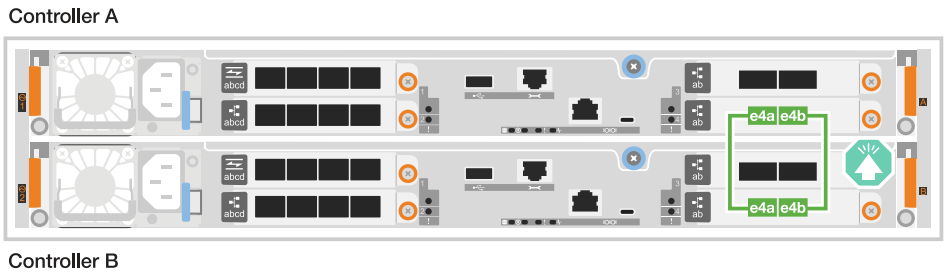
1. Conete as conexões de interconexão cluster/HA:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 10/25 GbE.

a. Conete a porta e4a do controlador A à porta e4a do controlador B.

b. Conete a porta e4b do controlador A à porta e4b do controlador B.

Cabos de interconexão de cluster/HA de 25 GbE



Cabeamento de cluster comutado

Conete os controladores aos switches de rede do cluster para criar as conexões do cluster ONTAP.

ASA A30 ou ASA A50 com dois módulos de e/S de 40/100 GbE de 2 portas

Passos

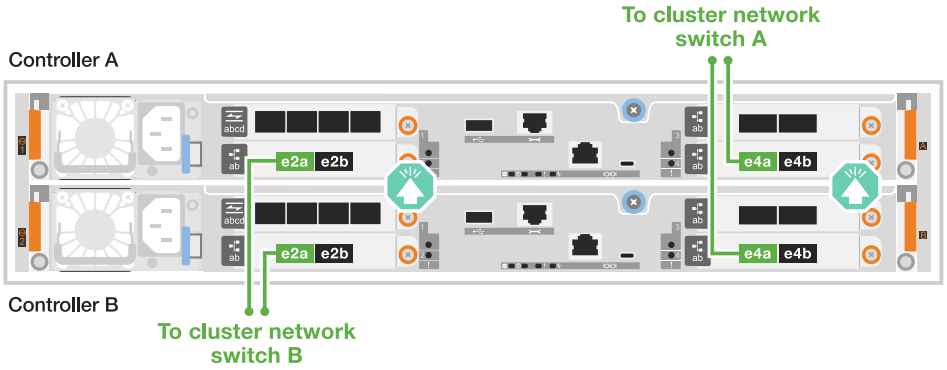
1. Cable as conexões de interconexão cluster/HA:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (nos módulos de e/S nos slots 2 e 4). As portas são de 40/100 GbE.

a. Conecte a porta e4a do controlador A ao switch de rede do cluster A.
b. Conecte a porta e2a do controlador A ao switch de rede do cluster B.
c. Conecte a porta e4a do controlador B ao switch de rede do cluster A.
d. Conecte a porta e2a do controlador B ao switch de rede do cluster B.

> As portas E2B e e4b do módulo de e/S não são utilizadas e estão disponíveis para conetividade de rede de host.

Cabos de interconexão de cluster/HA de 40/100 GbE



ASA A30 ou ASA A50 com um módulo de e/S de 40/100 GbE de 2 portas

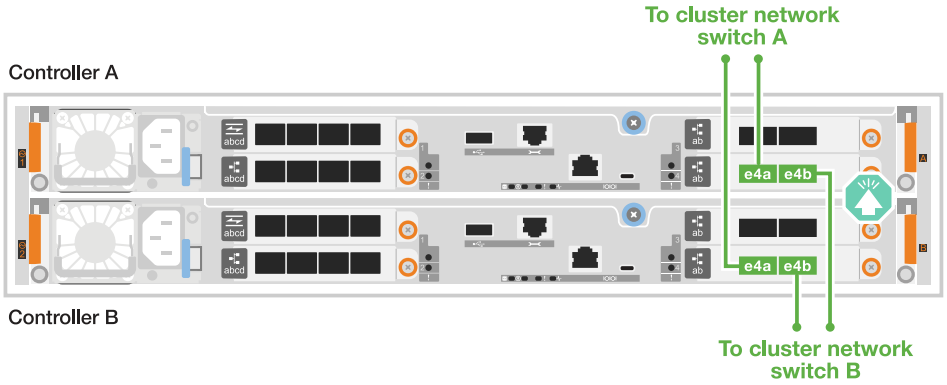
Passos

1. Faça o cabo dos controladores para os switches de rede do cluster:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 40/100 GbE.

a. Conecte a porta e4a do controlador A ao switch de rede do cluster A.
b. Conecte a porta e4b do controlador A ao switch de rede do cluster B.
c. Conecte a porta e4a do controlador B ao switch de rede do cluster A.
d. Conecte a porta e4b do controlador B ao switch de rede do cluster B.

Cabos de interconexão de cluster/HA de 40/100 GbE



ASA A20 com um módulo de e/S de 10/25 GbE de 2 portas

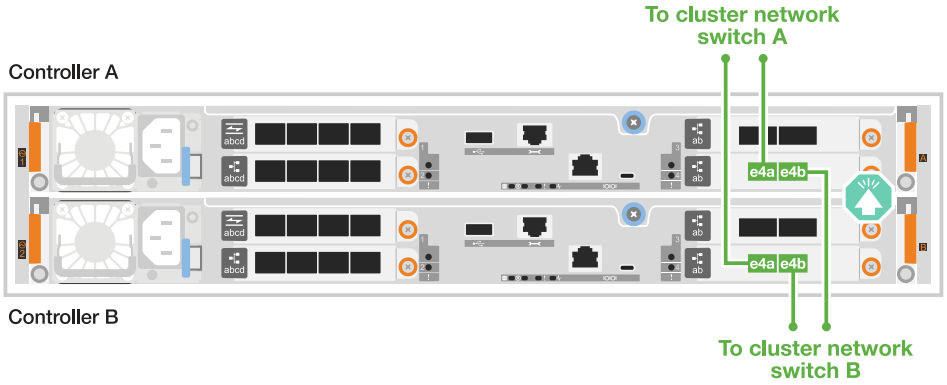
1. Faça o cabo dos controladores para os switches de rede do cluster:

   O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 10/25 GbE.

   a. Conecte a porta e4a do controlador A ao switch de rede do cluster A.
   b. Conecte a porta e4b do controlador A ao switch de rede do cluster B.
   c. Conecte a porta e4a do controlador B ao switch de rede do cluster A.
   d. Conecte a porta e4b do controlador B ao switch de rede do cluster B.

   Cabos de interconexão de cluster/HA de 10/25 GbE

Crie as conexões do cluster do ONTAP. Para clusters sem switch, conecte as controladoras umas às outras. Para clusters comutados, conete os controladores aos switches de rede do cluster.

Os exemplos de cabeamento de cluster/HA mostram configurações comuns.

Se você não vê sua configuração aqui, vá para "NetApp Hardware Universe" para obter informações abrangentes sobre configuração e prioridade de slots para cabear seu sistema de armazenamento.

Cabeamento de cluster sem switch

Conete os controladores uns aos outros para criar as conexões do cluster do ONTAP.

ASA C30 com dois módulos de E/S 40/100 GbE de 2 portas

Passos

1. Cable as conexões de interconexão cluster/HA:

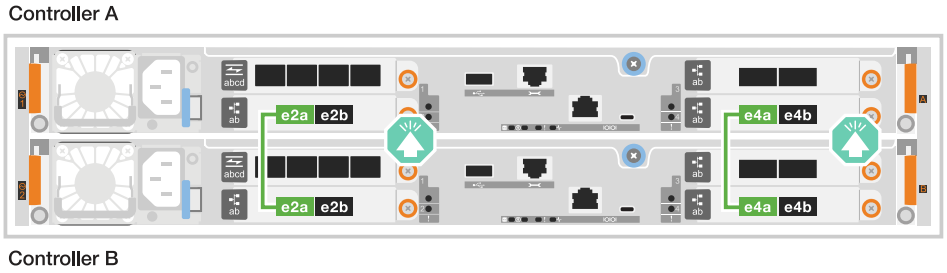
> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (nos módulos de e/S nos slots 2 e 4). As portas são de 40/100 GbE.

a. Conete a porta E2A do controlador A à porta E2A do controlador B.

b. Conete a porta e4a do controlador A à porta e4a do controlador B.

> As portas E2B e e4b do módulo de e/S não são utilizadas e estão disponíveis para conetividade de rede de host.

Cabos de interconexão de cluster/HA de 100 GbE



ASA C30 com um módulo de e/S de 40/100 GbE de 2 portas

Passos

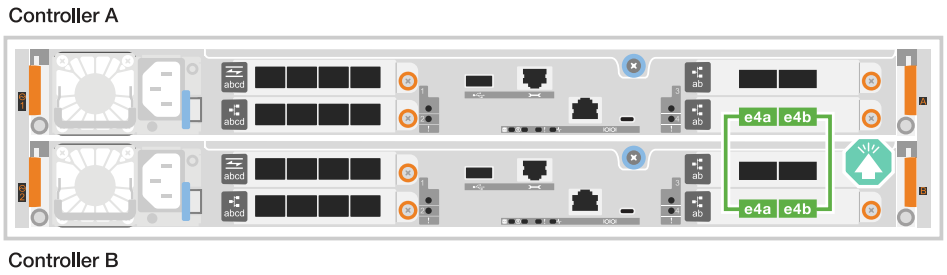
1. Cable as conexões de interconexão cluster/HA:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 40/100 GbE.

a. Conete a porta e4a do controlador A à porta e4a do controlador B.

b. Conete a porta e4b do controlador A à porta e4b do controlador B.

Cabos de interconexão de cluster/HA de 100 GbE



Cabeamento de cluster comutado

Conete os controladores aos switches de rede do cluster para criar as conexões do cluster ONTAP.

ASA C30 com dois módulos de E/S 40/100 GbE de 2 portas

Passos

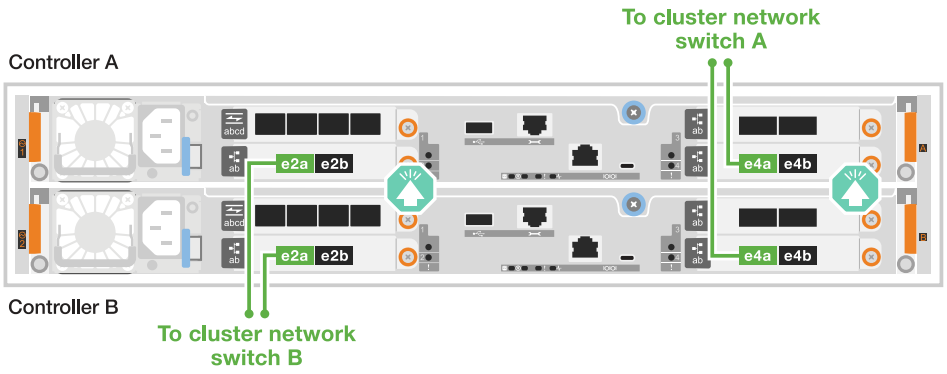
1. Cable as conexões de interconexão cluster/HA:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (nos módulos de e/S nos slots 2 e 4). As portas são de 40/100 GbE.

a. Conecte a porta e4a do controlador A ao switch de rede do cluster A.
b. Conecte a porta e2a do controlador A ao switch de rede do cluster B.
c. Conecte a porta e4a do controlador B ao switch de rede do cluster A.
d. Conecte a porta e2a do controlador B ao switch de rede do cluster B.

> As portas E2B e e4b do módulo de e/S não são utilizadas e estão disponíveis para conetividade de rede de host.

Cabos de interconexão de cluster/HA de 40/100 GbE



ASA C30 com um módulo de e/S de 40/100 GbE de 2 portas

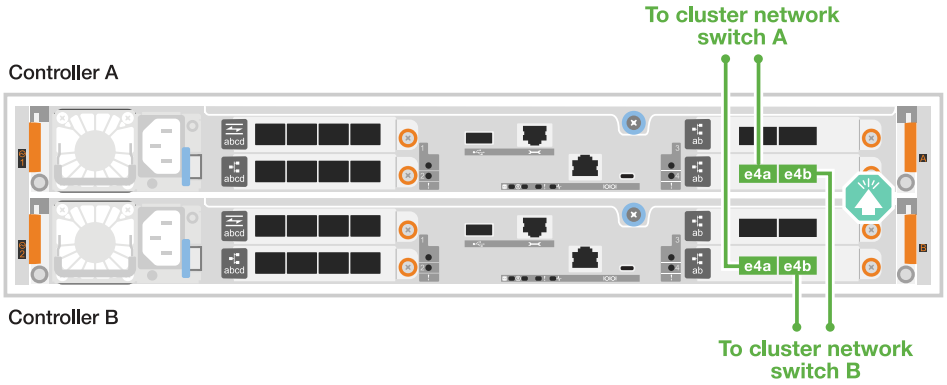
Passos

1. Conecte os controladores aos switches da rede do cluster:

> O tráfego de interconexão de cluster e o tráfego de HA compartilham as mesmas portas físicas (no módulo de e/S no slot 4). As portas são de 40/100 GbE.

a. Conecte a porta e4a do controlador A ao switch de rede do cluster A.
b. Conecte a porta e4b do controlador A ao switch de rede do cluster B.
c. Conecte a porta e4a do controlador B ao switch de rede do cluster A.
d. Conecte a porta e4b do controlador B ao switch de rede do cluster B.

Cabos de interconexão de cluster/HA de 40/100 GbE



Etapa 2: Faça o cabeamento das conexões de rede do host

Conete os controladores à rede host.

Este procedimento difere dependendo do modelo do sistema de armazenamento e da configuração do módulo de e/S.

A1K

Conete as portas do módulo Ethernet à rede host.

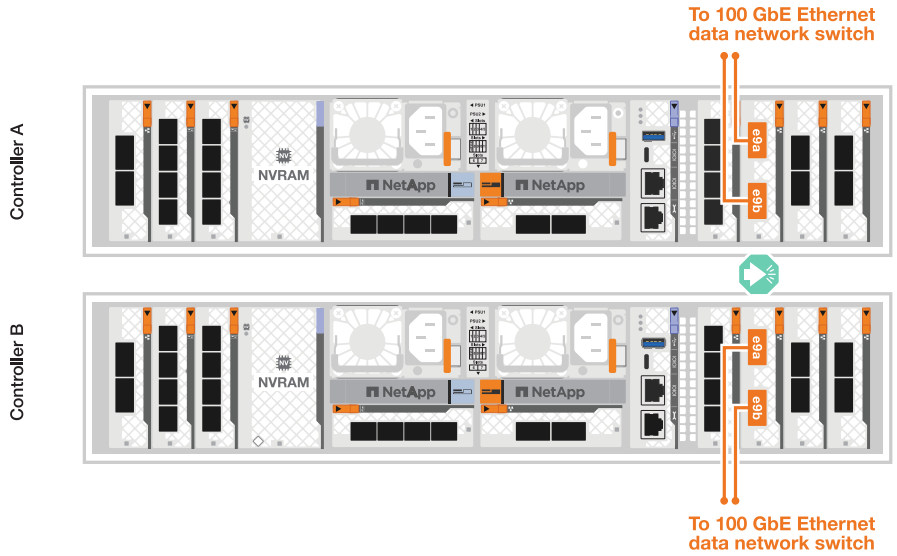
A seguir estão alguns exemplos típicos de cabeamento de rede de host. Consulte "NetApp Hardware Universe" para obter a configuração específica do sistema.

Passos

1. Conete as portas e9a e e9b ao switch de rede de dados Ethernet.

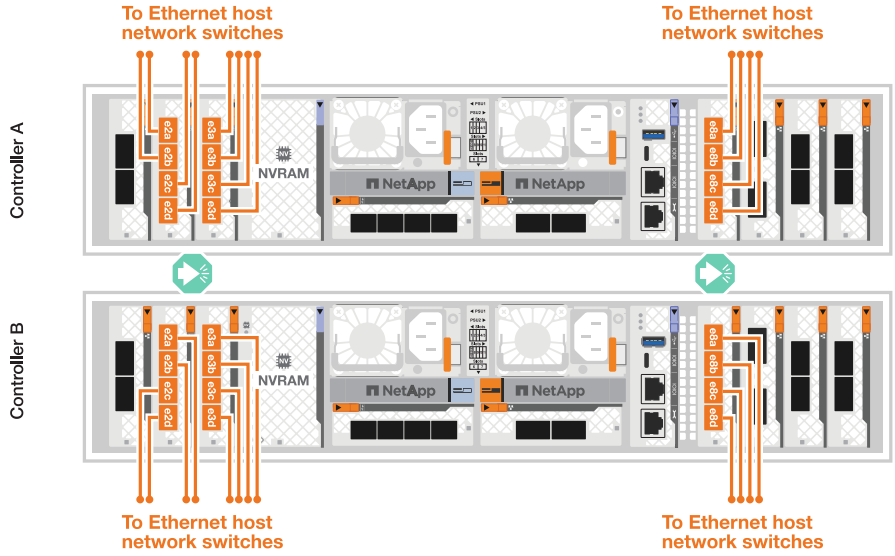
> Para obter o máximo desempenho do sistema para tráfego de cluster e HA, não use as portas e1b e E7B para conexões de rede de host. Use uma placa de host separada para maximizar o desempenho.

Cabo de 100 GbE



2. Conete seus switches de rede host de 10/25 GbE.

Host de 10/25 GbE



A70 e A90

Conete as portas do módulo Ethernet à rede host.

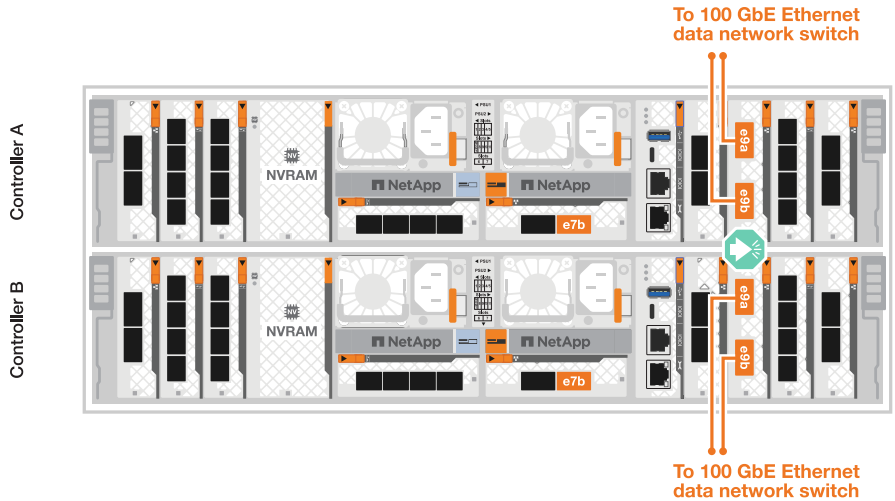
A seguir estão alguns exemplos típicos de cabeamento de rede de host. Consulte "NetApp Hardware Universe" para obter a configuração específica do sistema.

Passos

1. Conete as portas e9a e e9b ao switch de rede de dados Ethernet.

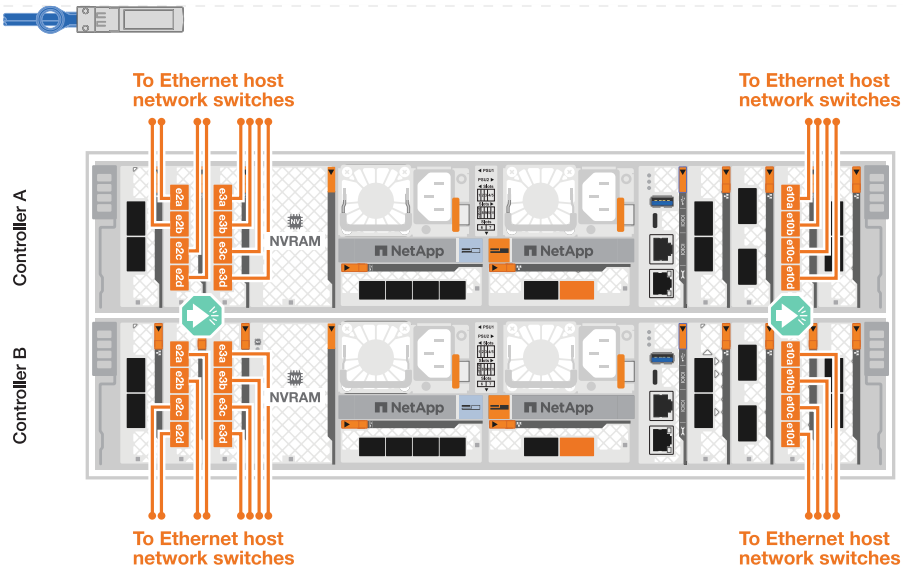
> Para obter o máximo desempenho do sistema para tráfego de cluster e HA, não use as portas e1b e E7B para conexões de rede de host. Use uma placa de host separada para maximizar o desempenho.

Cabo de 100 GbE



2. Conete seus switches de rede host de 10/25 GbE.

Host de 4 portas e 10/25 GbE



A20, A30 E A50

Conete as portas do módulo Ethernet ou as portas do módulo Fibre Channel (FC) à rede do host.

Os exemplos de cabeamento de rede do host mostram configurações comuns.

Se você não vê sua configuração aqui, vá para "NetApp Hardware Universe" para obter informações abrangentes sobre configuração e prioridade de slots para cabear seu sistema de armazenamento.

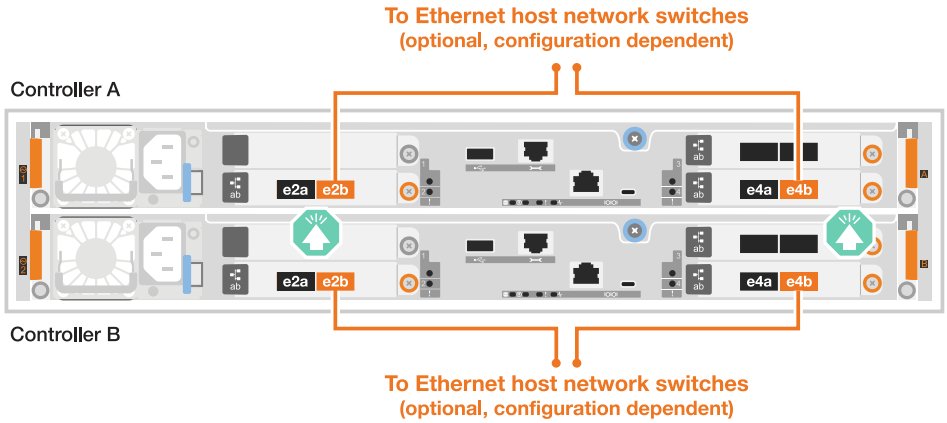
Cabeamento de host Ethernet

ASA A30 e ASA A50 com dois módulos de e/S de 40/100 GbE de 2 portas

Em cada controladora, conete as portas E2B e e4b aos switches de rede host Ethernet.

> As portas nos módulos de e/S no slot 2 e 4 são de 40/100 GbE (a conectividade de host é de 40/100 GbE).

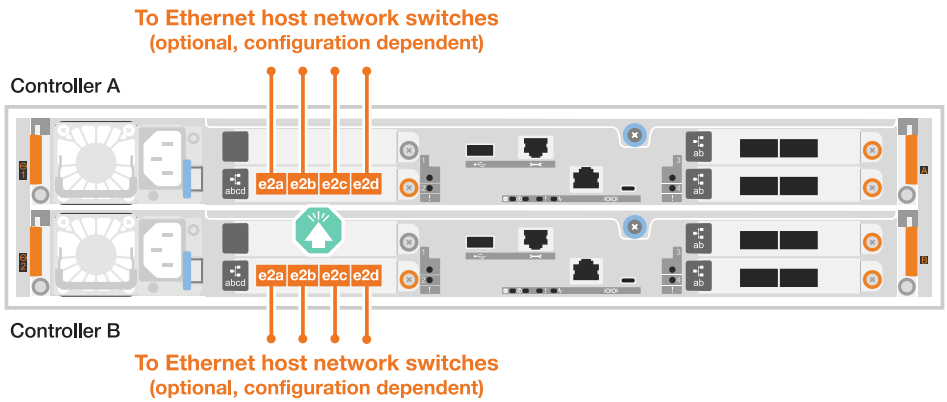
Cabos de 40/100 GbE



ASA A20, A30 e A50 com um módulo de E/S 10/25 GbE de 4 portas

Em cada controladora, conete as portas E2A, E2B, E2C e e2D aos switches de rede host Ethernet.

Cabos de 10/25 GbE

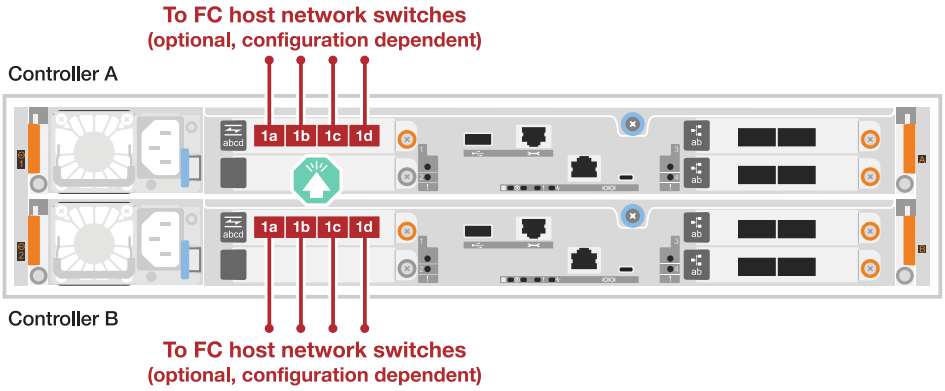


Cabeamento de host FC

ASA A20, A30 e A50 com um módulo de E/S FC de 4 portas e 64 Gb/s

Em cada controlador, conecte as portas 1a, 1b, 1c e 1D aos switches de rede de host FC.

Cabos FC de 64 GB/s



Conete as portas do módulo Ethernet ou as portas do módulo Fibre Channel (FC) à rede do host.

Os exemplos de cabeamento de rede do host mostram configurações comuns.

Se você não vê sua configuração aqui, vá para "NetApp Hardware Universe" para obter informações abrangentes sobre configuração e prioridade de slots para cabear seu sistema de armazenamento.

Cabeamento de host Ethernet

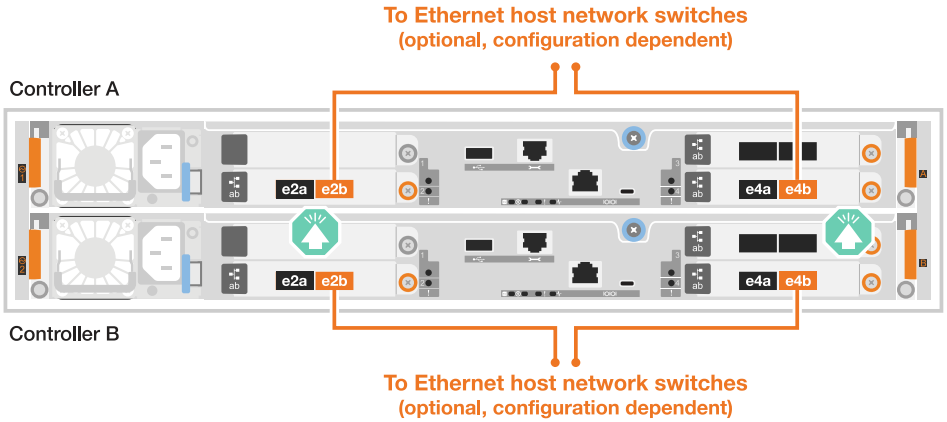
ASA C30 com dois módulos de E/S 40/100 GbE de 2 portas

Passos

1. Em cada controladora, as portas de cabo E2B e e4b para os switches de rede host Ethernet.

> As portas nos módulos de e/S no slot 2 e 4 são de 40/100 GbE (a conectividade de host é de 40/100 GbE).

Cabos de 40/100 GbE

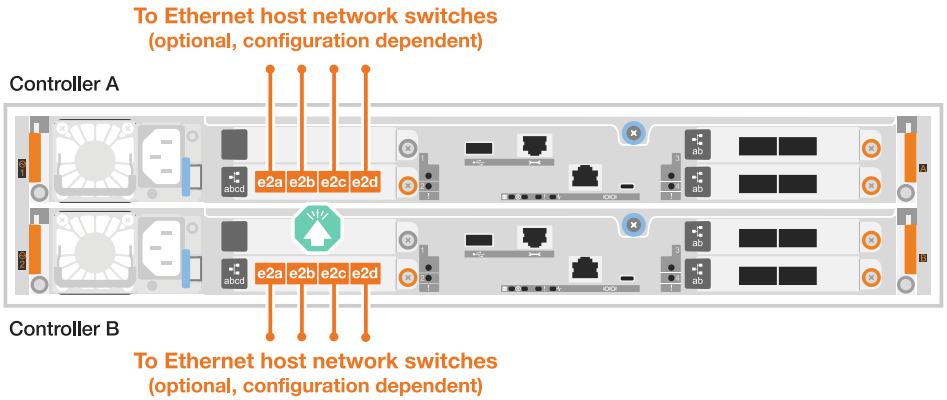


ASA C30 com um módulo de e/S de 10/25 GbE de 4 portas

Passos

1. Em cada controlador, as portas de cabo E2A, E2B, E2C e e2D para os switches de rede de host Ethernet.

Cabos de 10/25 GbE

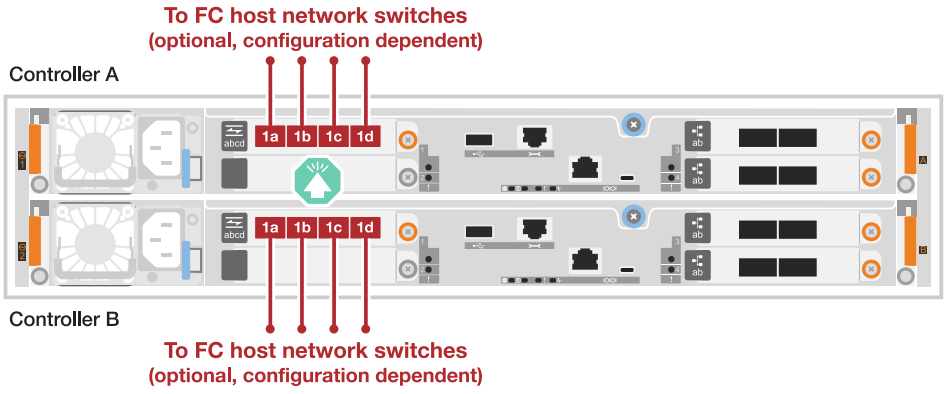


ASA C30 com um módulo de E/S FC de 4 portas e 64 Gb/s

Passos

1. Em cada controladora, cable as portas 1a, 1b, 1c e 1D para os switches de rede de host FC.

Cabos FC de 64 GB/s



Passo 3: Faça o cabeamento das conexões de rede de gerenciamento

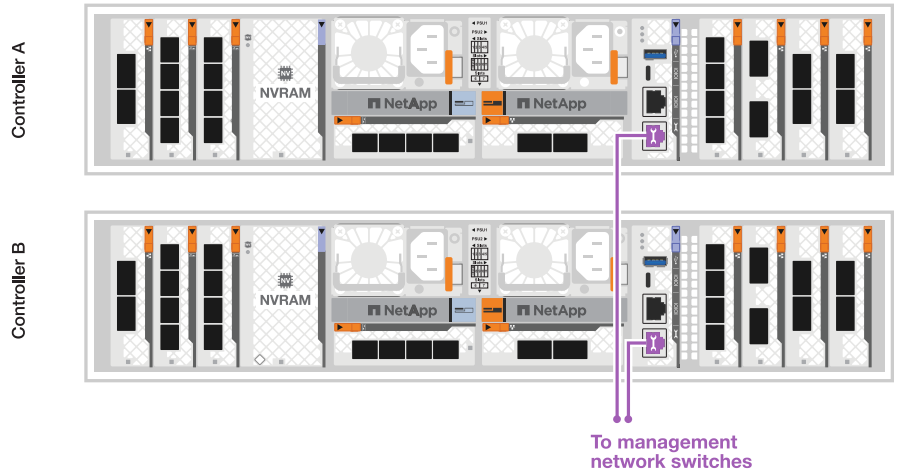
Conete os controladores à sua rede de gerenciamento.

Contacte o administrador da rede para obter informações sobre como ligar o sistema de armazenamento aos comutadores de rede de gestão.

A1K

Use os cabos RJ-45 de 1000BASEBASE-T para conetar as portas de gerenciamento (chave inglesa) em cada controlador aos switches de rede de gerenciamento.

CABOS RJ-45 DE 1000BASEBASE-T

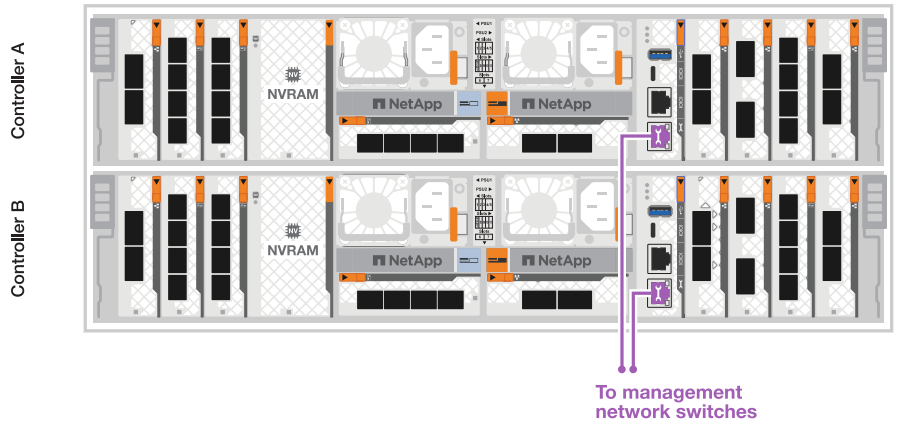


Não conete os cabos de energia ainda.

A70 e A90

Use os cabos RJ-45 de 1000BASEBASE-T para conetar as portas de gerenciamento (chave inglesa) em cada controlador aos switches de rede de gerenciamento.

CABOS RJ-45 DE 1000BASEBASE-T

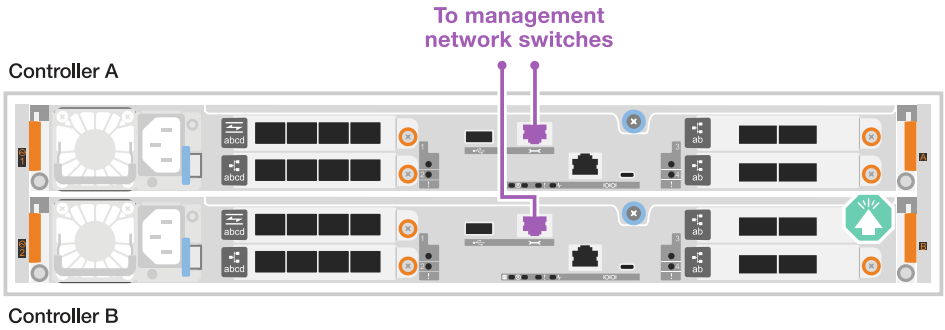


Não conete os cabos de energia ainda.

A20, A30 E A50

Conete as portas de gerenciamento (chave inglesa) em cada controlador aos switches de rede de gerenciamento.

CABOS RJ-45 DE 1000BASEBASE-T

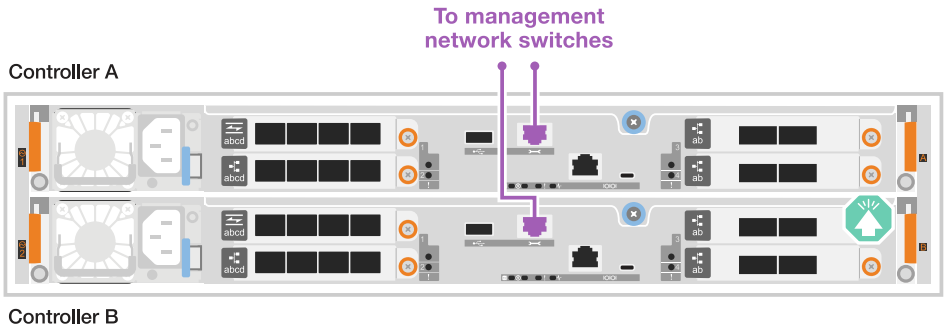


Não conete os cabos de energia ainda.

C30

Conete as portas de gerenciamento (chave inglesa) em cada controlador aos switches de rede de gerenciamento.

CABOS RJ-45 DE 1000BASEBASE-T



Não conete os cabos de energia ainda.

Etapa 4: Faça o cabeamento das conexões da prateleira

Os procedimentos de cabeamento a seguir mostram como conectar suas controladoras a um compartimento de storage.

Para obter o número máximo de gavetas compatíveis com o seu sistema de storage e para todas as opções de cabeamento, como ótico e conectado a switch, "NetApp Hardware Universe"consulte .

A1K

Os sistemas de armazenamento AFF A1K suportam prateleiras NS224 com o módulo NSM100 ou NSM100B. As principais diferenças entre os módulos são:

- Os módulos de prateleira NSM100 usam portas e0a e e0b integradas.
- Os módulos de prateleira NSM100B usam as portas e1a e e1b no slot 1.

O exemplo de cabeamento a seguir mostra módulos NSM100 nas prateleiras NS224 ao se referir às portas do módulo de prateleira.

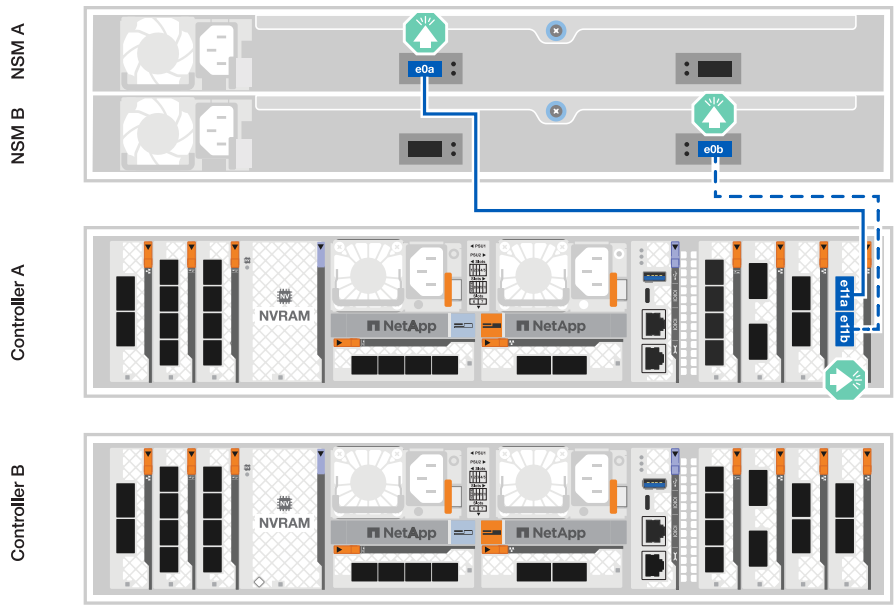
Escolha uma das seguintes opções de cabeamento que corresponda à sua configuração.

Opção 1: Uma gaveta de armazenamento de NS224 GB

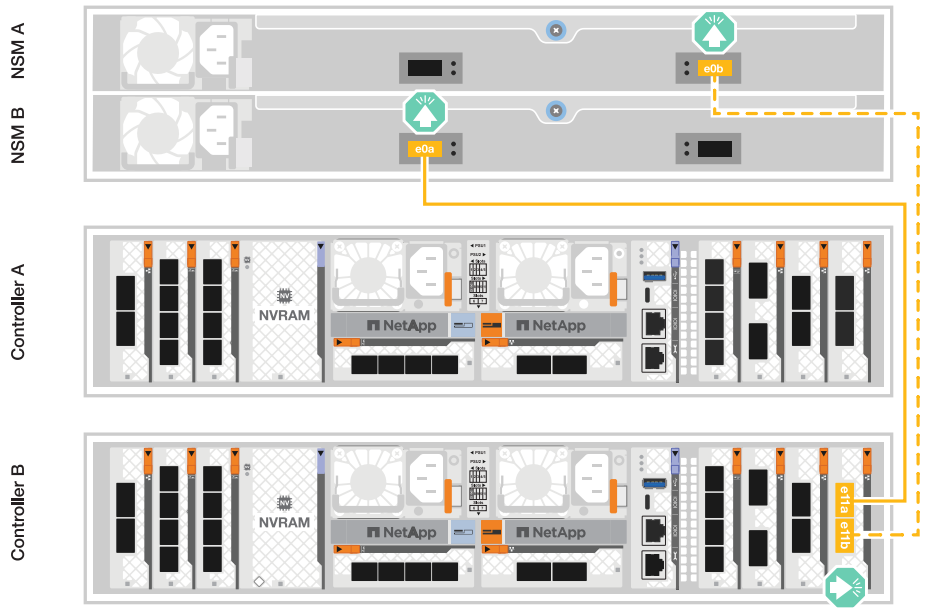
Conete cada controlador aos módulos NSM no compartimento NS224. Os gráficos mostram o cabeamento de cada uma das controladoras: O cabeamento da controladora A é exibido em azul e o cabeamento da controladora B é exibido em amarelo.

Passos

1. No controlador A, ligue as seguintes portas:
   a. Conete a porta e11a à porta NSM A e0a.
   b. Conete a porta e11b à porta NSM B e0b.



2. No controlador B, ligue as seguintes portas:
   a. Conete a porta e11a à porta NSM B e0a.
   b. Conete a porta e11b à porta NSM A e0b.

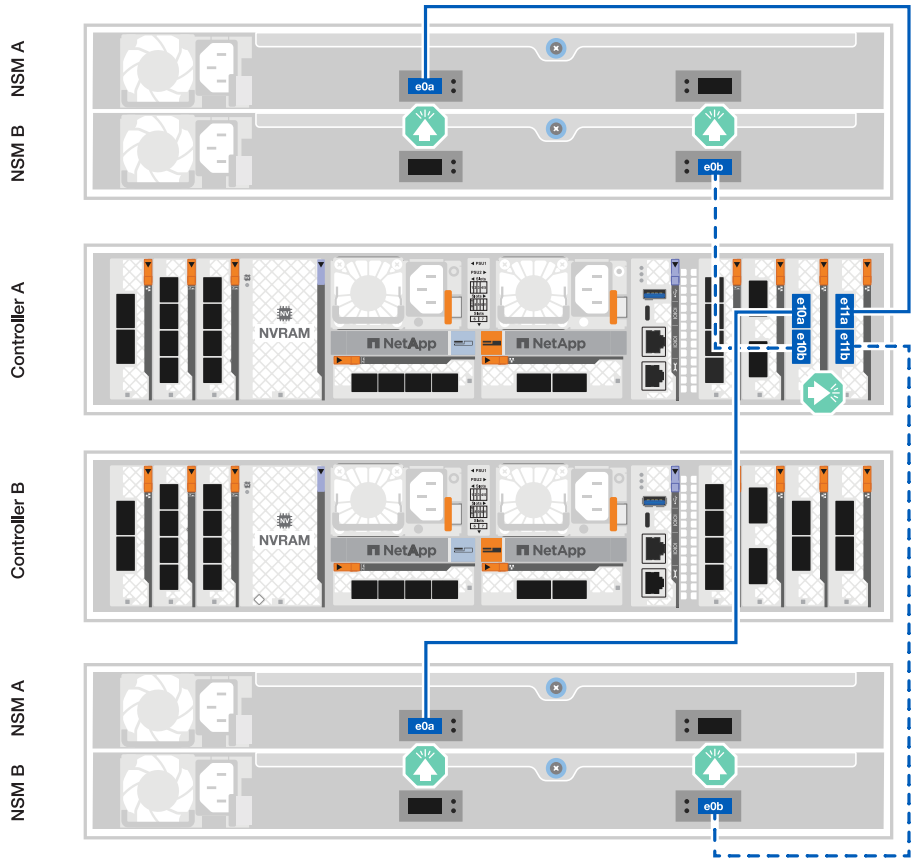


Opção 2: Duas prateleiras de armazenamento NS224

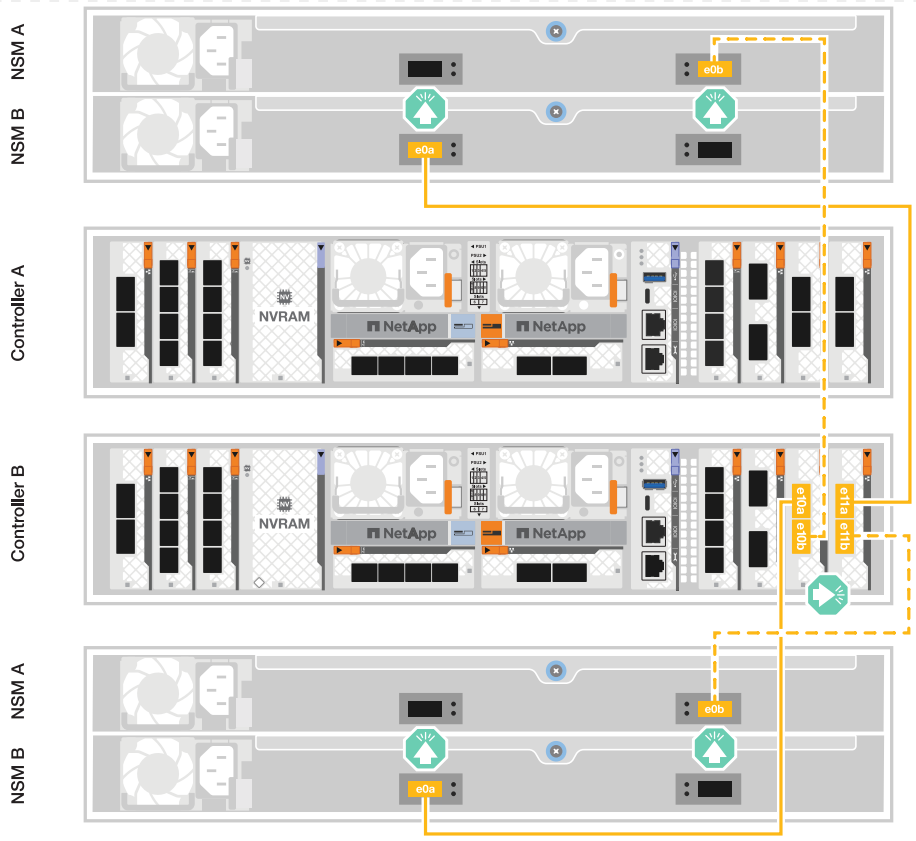
Conecte cada controladora aos módulos do NSM nas duas gavetas NS224. Os gráficos mostram o cabeamento de cada uma das controladoras: O cabeamento da controladora A é exibido em azul e o cabeamento da controladora B é exibido em amarelo.

Passos

1. No controlador A, ligue as seguintes portas:
   a. Conete a porta e11a ao compartimento 1 NSM A porta e0a.
   b. Conete a porta e11b à porta e0b do NSM B da gaveta 2.
   c. Conete a porta e10a ao compartimento 2 NSM A porta e0a.
   d. Conete a porta e10b ao compartimento 1 NSM A porta e0b.



2. No controlador B, ligue as seguintes portas:
   a. Conete a porta e11a à porta e0a do NSM B da gaveta 1.
   b. Conete a porta e11b ao compartimento 2 NSM A porta e0b.
   c. Conete a porta e10a à porta e0a do NSM B da gaveta 2.
   d. Conete a porta e10b ao compartimento 1 NSM A porta e0b.



A70 e A90

Os sistemas de armazenamento AFF A70 e 90 suportam prateleiras NS224 com o módulo NSM100 ou NSM100B. As principais diferenças entre os módulos são:

- Os módulos de prateleira NSM100 usam portas integradas e0a e e0b.
- Os módulos de prateleira NSM100B usam as portas e1a e e1b no slot 1.

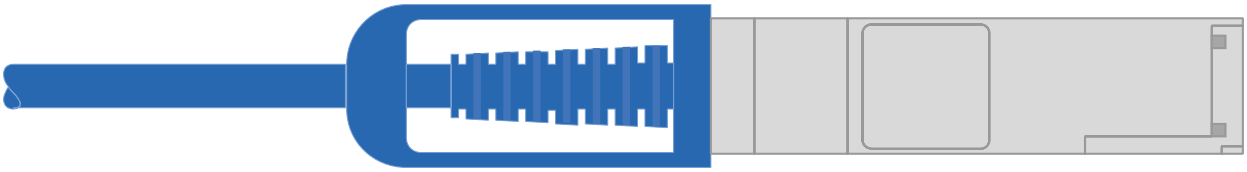
O exemplo de cabeamento a seguir mostra módulos NSM100 nas prateleiras NS224 ao se referir às portas do módulo de prateleira.

Escolha uma das seguintes opções de cabeamento que corresponda à sua configuração.

Opção 1: Uma gaveta de armazenamento de NS224 GB

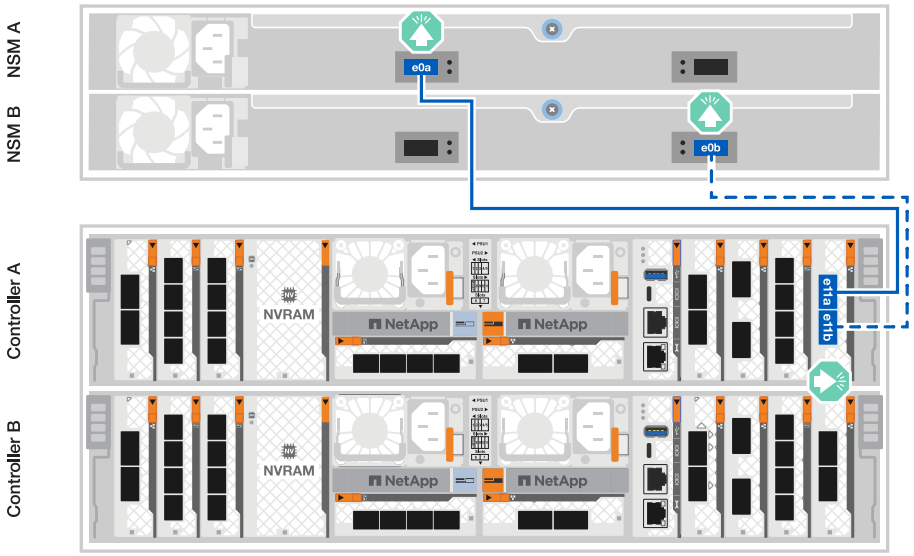
Conete cada controlador aos módulos NSM no compartimento NS224. Os gráficos mostram o cabeamento de cada uma das controladoras: O cabeamento da controladora A é exibido em azul e o cabeamento da controladora B é exibido em amarelo.

Cabos de cobre 100 GbE QSFP28

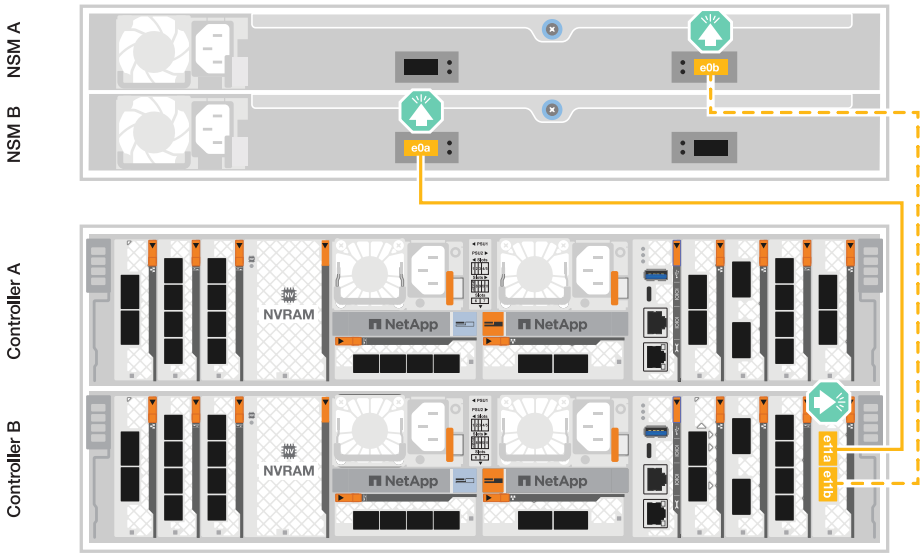


Passos

1. Conete a porta e11a do controlador A à porta e0a do NSM A.
2. Conete a porta e11b do controlador A à porta e0b do NSM B.



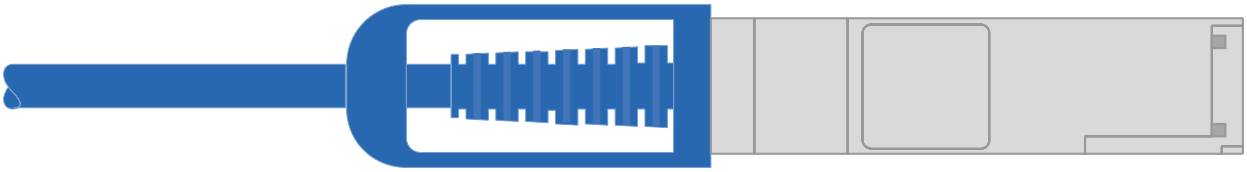
3. Conete a porta e11a do controlador B à porta e0a do NSM B.
4. Conete a porta e11b do controlador B à porta e0b do NSM A.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e11a
e11b

Opção 2: Duas prateleiras de armazenamento NS224

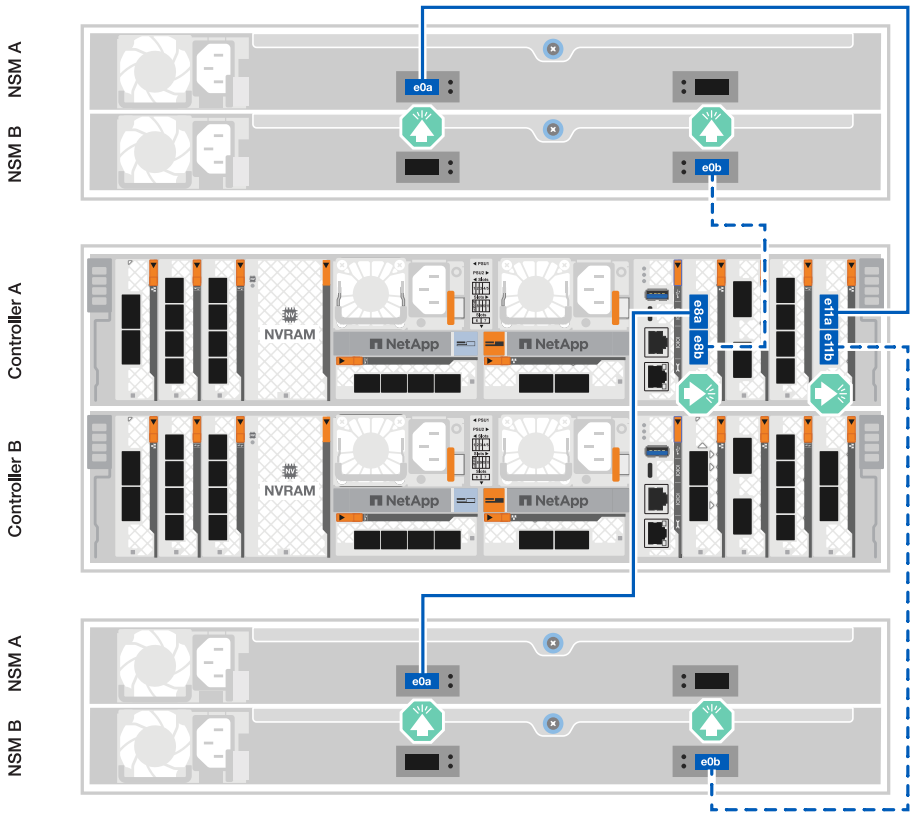
Conecte cada controladora aos módulos do NSM nas duas gavetas NS224. Os gráficos mostram o cabeamento de cada uma das controladoras: O cabeamento da controladora A é exibido em azul e o cabeamento da controladora B é exibido em amarelo.

Cabos de cobre 100 GbE QSFP28



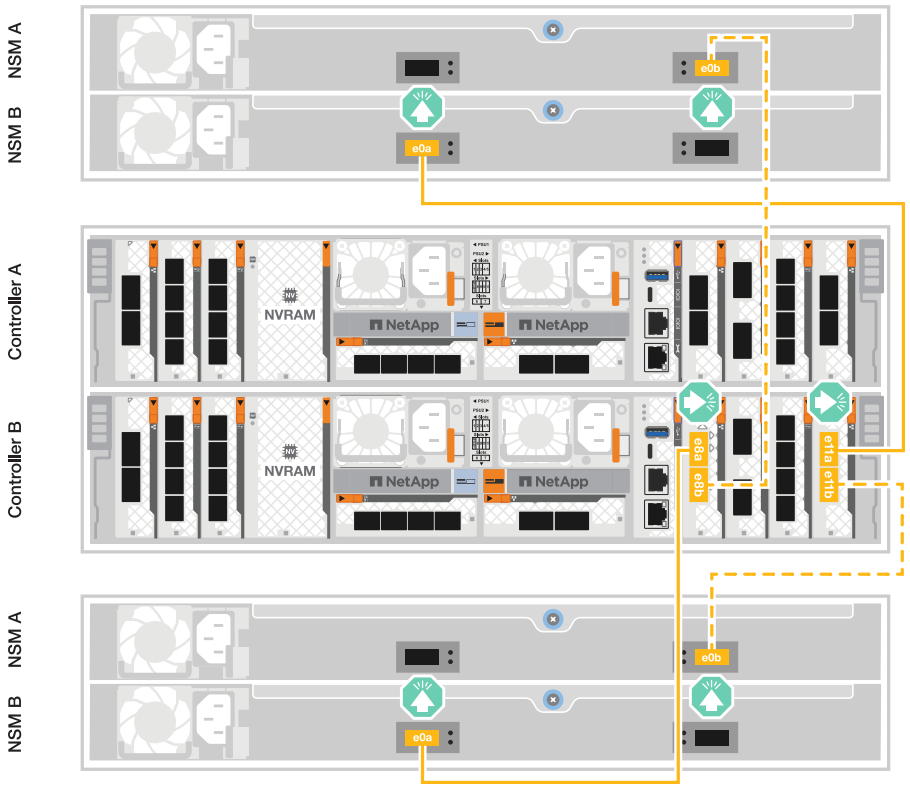
Passos

1. No controlador A, ligue as seguintes portas:
   a. Conete a porta e11a ao compartimento 1, NSM A porta e0a.
   b. Conete a porta e11b à gaveta 2, porta NSM B e0b.
   c. Conete a porta e8a ao compartimento 2, NSM A porta e0a.
   d. Conete a porta e8b à gaveta 1, porta NSM B e0b.



2. No controlador B, ligue as seguintes portas:
   a. Conete a porta e11a à gaveta 1, porta NSM B e0a.
   b. Conete a porta e11b ao compartimento 2, NSM A porta e0b.
   c. Conete a porta e8a à gaveta 2, porta NSM B e0a.

d. Conete a porta e8b ao compartimento 1, NSM A porta e0b.



A20, A30 E A50

O procedimento de cabeamento de prateleira NS224 mostra módulos NSM100B em vez de módulos NSM100. O cabeamento é o mesmo, independentemente do tipo de módulo NSM utilizado, apenas os nomes das portas são diferentes:

- Os módulos NSM100B usam as portas e1a e e1b em um módulo de E/S no slot 1.
- Os módulos NSM100 usam portas integradas (onboard) e0a e e0b.

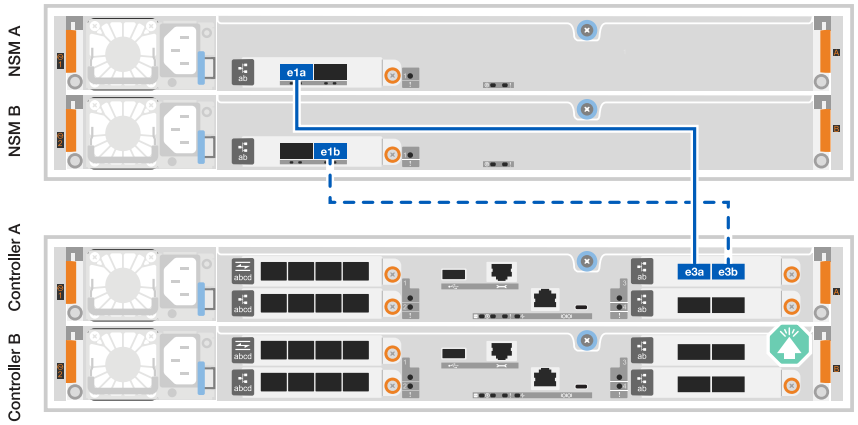
Você conecta cada controlador a cada módulo NSM na prateleira NS224 usando os cabos de armazenamento fornecidos com seu sistema de armazenamento, que podem ser do seguinte tipo de cabo:

Cabos de cobre 100 GbE QSFP28

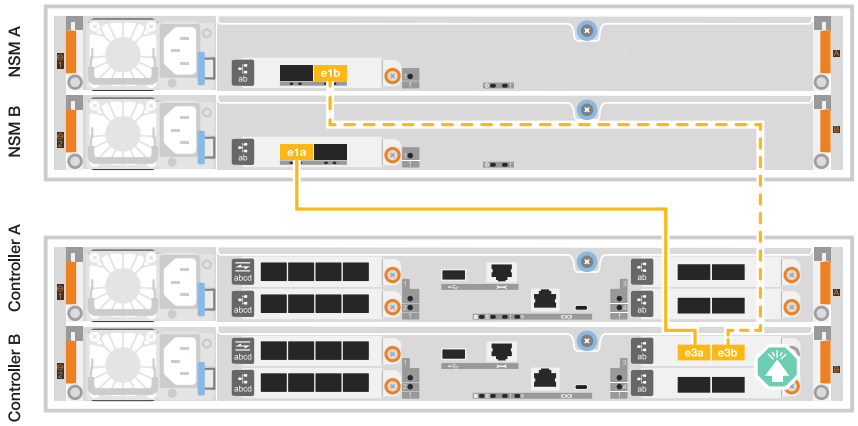
Os gráficos mostram o cabeamento A do controlador em azul e o cabeamento B do controlador em amarelo.

Passos

1. Conete o controlador A à gaveta:
   a. Conete a porta e3a do controlador A à porta e1a do NSM A.
   b. Conete a porta e3b do controlador A à porta e1b do NSM B.



2. Conete o controlador B à prateleira:
   a. Conete a porta e3a do controlador B à porta e1a do NSM B.
   b. Conete a porta e3b do controlador B à porta e1b do NSM A.



C30

O procedimento de cabeamento de prateleira NS224 mostra módulos NSM100B em vez de módulos NSM100. O cabeamento é o mesmo, independentemente do tipo de módulo NSM utilizado, apenas os nomes das portas são diferentes:

- Os módulos NSM100B usam as portas e1a e e1b em um módulo de E/S no slot 1.
- Os módulos NSM100 usam portas integradas (onboard) e0a e e0b.

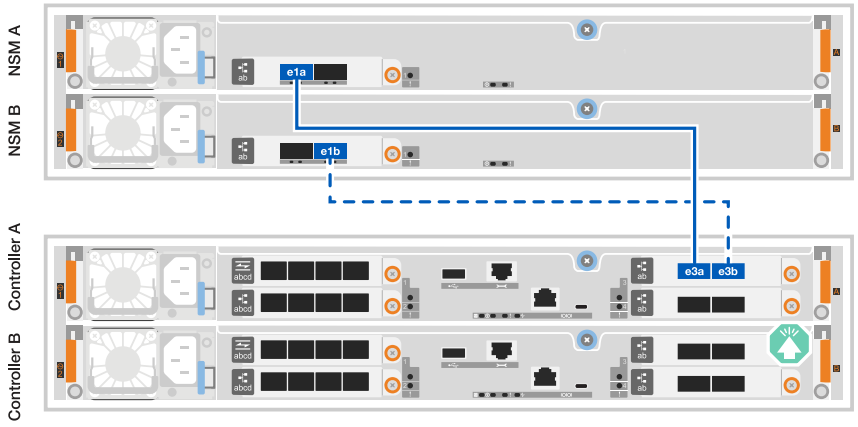
Você conecta cada controlador a cada módulo NSM na prateleira NS224 usando os cabos de armazenamento fornecidos com seu sistema de armazenamento, que podem ser do seguinte tipo de cabo:

Cabos de cobre 100 GbE QSFP28

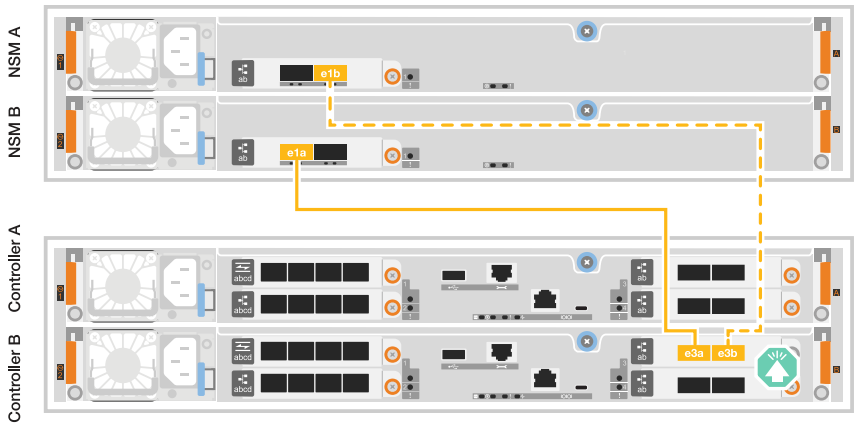
Os gráficos mostram o cabeamento A do controlador em azul e o cabeamento B do controlador em amarelo.

Passos

1. Conete o controlador A à gaveta:
   a. Conete a porta e3a do controlador A à porta e1a do NSM A.
   b. Conete a porta e3b do controlador A à porta e1b do NSM B.



2. Conete o controlador B à prateleira:
   a. Conete a porta e3a do controlador B à porta e1a do NSM B.
   b. Conete a porta e3b do controlador B à porta e1b do NSM A.



O que se segue?

Depois de conectar os controladores de storage à rede e, em seguida, conectá-los às gavetas de storage, você "Ligue o sistema de armazenamento ASA r2".

Ligue o sistema de storage ASA R2

Depois de instalar o hardware de rack para seu sistema de storage ASA r2 e instalar os cabos das controladoras e gavetas de storage, ligue as controladoras e gavetas de storage.

Etapa 1: Ligue a prateleira e atribua o ID da prateleira

Cada prateleira é distinguida por um ID de prateleira exclusivo. Esse ID garante que o compartimento seja distinto na configuração do sistema de storage.

Sobre esta tarefa

- Um ID válido do compartimento é de 01 a 99.

  Se você tiver compartimentos internos (storage), que estão integrados às controladoras, receberá um ID de compartimento fixo de 00 GB a elas.

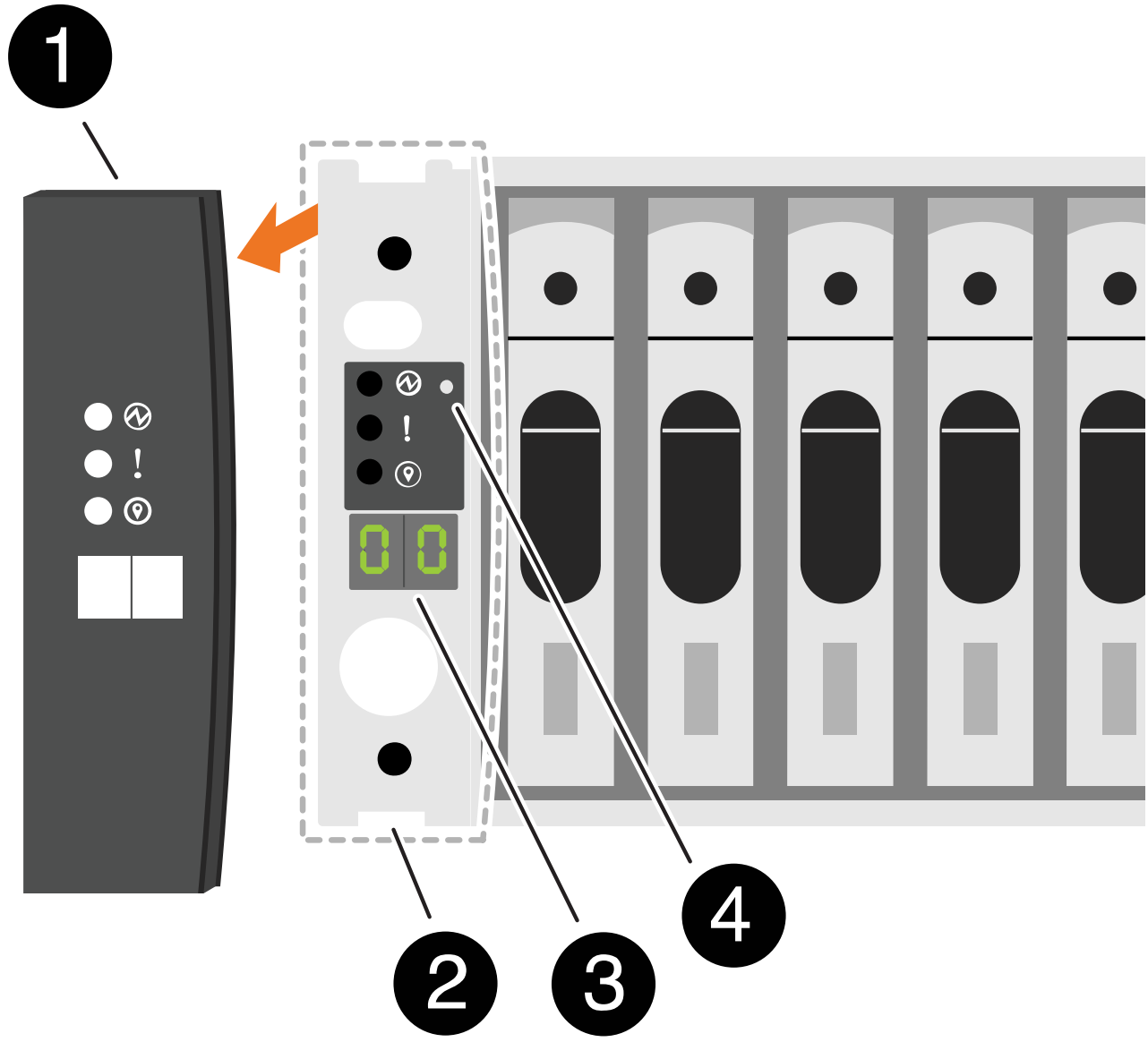
- É necessário desligar um compartimento (Desconete os dois cabos de energia, aguarde o tempo apropriado e, em seguida, conectá-los novamente) para que a ID do compartimento entre em vigor.

Passos

1. Ligue a gaveta conetando os cabos de alimentação primeiro à gaveta, prendendo-os no lugar com o retentor do cabo de alimentação e, em seguida, conetando os cabos de alimentação a fontes de alimentação em circuitos diferentes.

   A prateleira liga-se e arranca automaticamente quando ligada à fonte de alimentação.

2. Remova a tampa da extremidade esquerda para acessar o botão ID da prateleira atrás da placa frontal.



1	Tampa da extremidade da prateleira
2	Placa frontal da prateleira
3	Número de ID do compartimento
4	Botão ID do compartimento

3. Altere o primeiro número do ID do compartimento:
   a. Insira a extremidade reta de um clipe de papel ou caneta esferográfica com ponta fina no pequeno orifício para pressionar o botão ID da prateleira.
   b. Pressione e segure o botão ID do compartimento até que o primeiro número no visor digital pisque e solte o botão.

      Pode demorar até 15 segundos para o número piscar. Isto ativa o modo de programação da ID da prateleira.

      > Se a ID demorar mais de 15 segundos a piscar, prima e mantenha premido o botão ID da prateleira novamente, certificando-se de que o pressiona completamente.

   c. Pressione e solte o botão ID do compartimento para avançar o número até atingir o número desejado de 0 a 9.

      A duração de cada imprensa e liberação pode ser tão curta quanto um segundo.

   O primeiro número continua a piscar.

4. Altere o segundo número do ID do compartimento:
   a. Prima e mantenha premido o botão até o segundo número no visor digital piscar.

      Pode demorar até três segundos para o número piscar.

   O primeiro número no visor digital pára de piscar.
   a. Pressione e solte o botão ID do compartimento para avançar o número até atingir o número desejado de 0 a 9.

      O segundo número continua a piscar.

5. Bloqueie o número pretendido e saia do modo de programação premindo e mantendo premido o botão ID da prateleira até que o segundo número pare de piscar.

   Pode demorar até três segundos para o número parar de piscar.

   Ambos os números no visor digital começam a piscar e o LED âmbar acende-se após cerca de cinco segundos, alertando-o de que a ID pendente do compartimento ainda não entrou em vigor.

6. Ligue o compartimento por pelo menos 10 segundos para fazer com que o ID do compartimento entre em vigor.

a. Desconete o cabo de alimentação de ambas as fontes de alimentação da prateleira.
b. Aguarde 10 segundos.
c. Conete os cabos de alimentação de volta às fontes de alimentação do compartimento para concluir o ciclo de energia.

   Uma fonte de alimentação é ligada assim que o cabo de alimentação é ligado. O LED bicolor deve acender-se a verde.

7. Volte a colocar a tampa da extremidade esquerda.

Passo 2: Ligue os controladores

Depois de ativar os compartimentos de storage e atribuir a eles IDs exclusivos, ligue a energia dos controladores de storage.

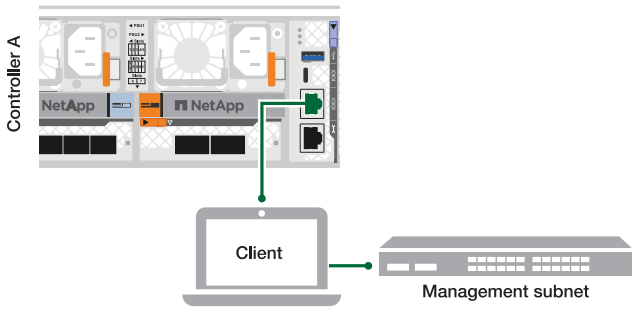
Passos

1. Ligue o computador portátil à porta da consola série. Isso permitirá que você monitore a sequência de inicialização quando os controladores estiverem ligados.
   a. Defina a porta do console serial no laptop para 115.200 baud com N-8-1.

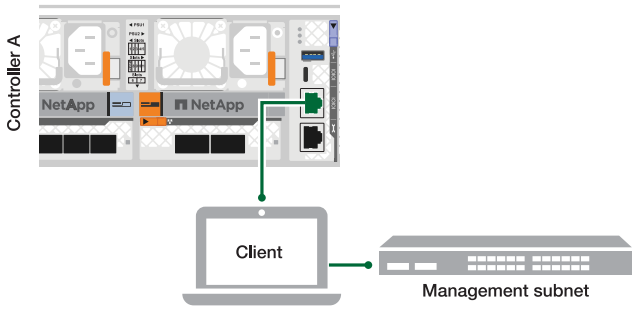
      Consulte a ajuda on-line do seu laptop para obter instruções sobre como configurar a porta do console serial.

   b. Conete o cabo do console ao laptop e conete a porta serial do console no controlador usando o cabo do console fornecido com o sistema de armazenamento.
   c. Conete o laptop ao switch na sub-rede de gerenciamento.

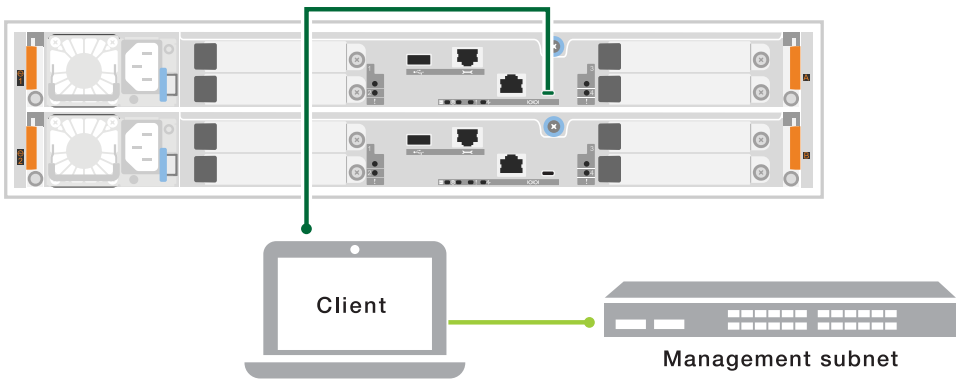
A1K



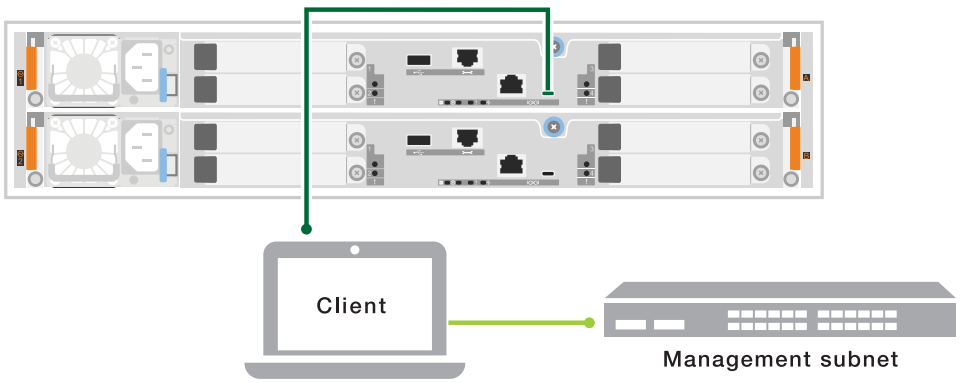
A70 e A90



A20, A30 E A50



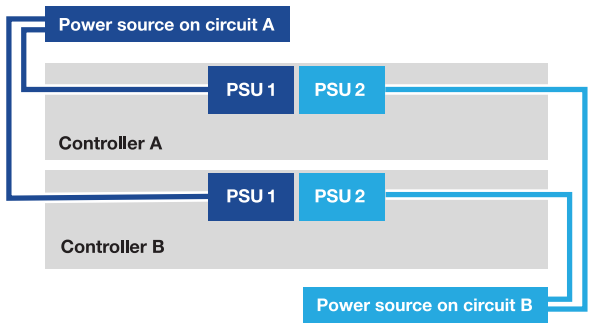
C30



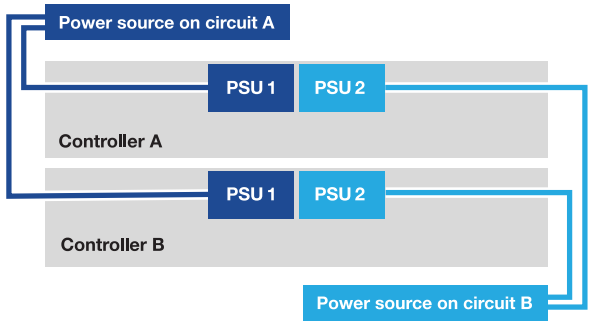
2. Atribua um endereço TCP/IP ao laptop, usando um que esteja na sub-rede de gerenciamento.
3. Conete os cabos de alimentação às fontes de alimentação do controlador e, em seguida, conete-os a

fontes de alimentação em diferentes circuitos.

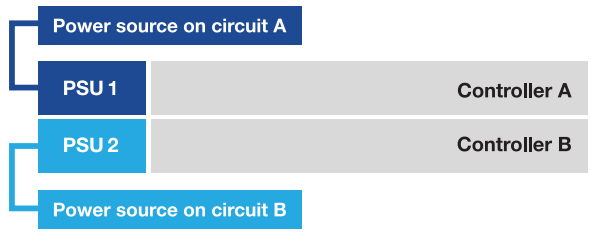
A1K



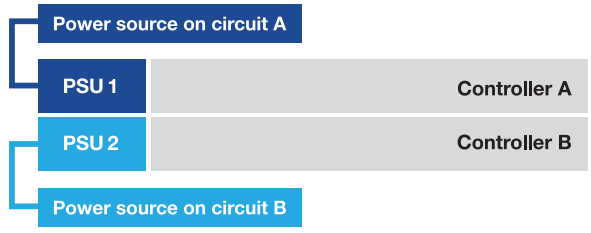
A70 e A90



A20, A30 E A50



C30



- O sistema inicia o processo de inicialização. A sequência de arranque inicial pode demorar até oito minutos.
- Durante o processo de inicialização, você observará os LEDs piscando e os ventiladores ativando, sinalizando que os controladores estão ligando.
- Esteja ciente de que os ventiladores podem emitir um alto nível de ruído quando iniciarem pela primeira vez. O ruído da ventoinha durante o arranque é normal.
- Para os sistemas de armazenamento ASA A20, A30, A50 e ASA C30, o visor de ID da prateleira na parte frontal do chassi do sistema não acende.

4. Fixe os cabos de alimentação usando o dispositivo de fixação em cada fonte de alimentação.

O que se segue?

Depois de ativar o sistema de armazenamento ASA r2, "Configure um cluster ONTAP ASA R2"você .

Configure o seu sistema ASA R2

Configure um cluster ONTAP no sistema de storage ASA R2

O Gerenciador de sistema do ONTAP orienta você por um fluxo de trabalho rápido e fácil para configurar um cluster do ONTAP ASA R2.

Durante a configuração do cluster, sua máquina virtual de armazenamento de dados (VM) padrão é criada. Opcionalmente, você pode habilitar o DNS (Domain Name System) para resolver nomes de host, definir seu cluster para usar o NTP (Network Time Protocol) para sincronização de tempo e ativar a criptografia de dados em repouso.

Em certos casos, você poderá precisar de "Utilize a interface de linha de comando (CLI) do ONTAP para configurar seu cluster.". Você deve usar a CLI, por exemplo, se seus protocolos de segurança não permitirem que você conecte um laptop aos seus switches de gerenciamento ou se estiver usando um sistema operacional que não seja Windows.

Antes de começar

Reúna as seguintes informações:

- Endereço IP de gerenciamento de cluster

  O endereço IP de gerenciamento de cluster é um endereço IPv4 exclusivo para a interface de gerenciamento de cluster usada pelo administrador do cluster para acessar a VM de armazenamento de administrador e gerenciar o cluster. Você pode obter esse endereço IP do administrador responsável pela atribuição de endereços IP na sua organização.

- Máscara de sub-rede da rede

  Durante a configuração do cluster, a ONTAP recomenda um conjunto de interfaces de rede apropriadas para sua configuração. Você pode ajustar a recomendação, se necessário.

- Endereço IP do gateway de rede
- Endereço IP do nó do parceiro
- Nomes de domínio DNS
- Endereços IP do servidor de nomes DNS
- Endereços IP do servidor NTP
- Máscara de sub-rede de dados

Passos

1. Descubra a sua rede de cluster
   a. Ligue o computador portátil ao comutador de gestão e aceda aos computadores e dispositivos de rede.
   b. Abra o Explorador de ficheiros.

c. Selecione **rede**; em seguida, clique com o botão direito do rato e selecione **Atualizar**.
d. Selecione um dos ícones ONTAP; em seguida, aceite os certificados apresentados no ecrã.

   O System Manager é aberto.

2. Em **Senha**, crie uma senha forte para a conta de administrador.

   A senha deve ter pelo menos oito carateres e deve conter pelo menos uma letra e um número.

3. Volte a introduzir a palavra-passe para confirmar e, em seguida, selecione **continuar**.
4. Em **endereços de rede**, insira um nome de sistema de armazenamento ou aceite o nome padrão.

   Se você alterar o nome padrão do sistema de armazenamento, o novo nome deve começar com uma letra e deve ter menos de 44 carateres. Você pode usar um ponto (.), hífen (-) ou sublinhado (_) no nome.

5. Introduza o endereço IP de gestão do cluster, a máscara de sub-rede, o endereço IP do gateway e o endereço IP do nó do parceiro; em seguida, selecione **continuar**.
6. Em **Serviços de rede**, selecione as opções desejadas para **usar o sistema de nomes de domínio (DNS) para resolver nomes de host** e para **usar o NTP (Network Time Protocol) para manter os tempos sincronizados**.

   Se optar por utilizar o DNS, introduza o domínio DNS e os servidores de nomes. Se optar por utilizar o NTP, introduza os servidores NTP; em seguida, selecione **continuar**.

7. Em **Encryption**, introduza uma frase-passe para o Onboard Key Manager (OKM).

   A criptografia de dados em repouso usando um OKM (Onboard Key Manager) é selecionada por padrão. Se pretender utilizar um gestor de chaves externo, atualize as seleções.

   Opcionalmente, você pode configurar seu cluster para criptografia após a conclusão da configuração do cluster.

8. Selecione **Inicializar**.

   Quando a configuração estiver concluída, você será redirecionado para o endereço IP de gerenciamento do cluster.

9. Em **rede**, selecione **Configurar protocolos**.

Para configurar IP (iSCSI e NVMe/TCP), faça isso…	Para configurar FC e NVMe/FC, faça isso…
a. Selecione **IP**; em seguida, selecione **Configurar interfaces IP**. b. Selecione **Adicionar uma sub-rede**. c. Introduza um nome para a sub-rede e, em seguida, introduza os endereços IP da sub-rede. d. Insira a máscara de sub-rede e, opcionalmente, insira um gateway; em seguida, selecione **Add**. e. Selecione a sub-rede que acabou de criar; em seguida, selecione **Guardar**. f. Selecione **Guardar**.	a. Selecione **FC**; em seguida, selecione **Configurar interfaces FC** e/ou **Configurar interfaces NVMe/FC**. b. Selecione as portas FC e/ou NVMe/FC; em seguida, selecione **Guardar**.

10. Opcionalmente, baixe e execute "ActiveIQ Config Advisor" para confirmar sua configuração.

    O ActiveIQ Config Advisor é uma ferramenta para sistemas NetApp que verifica erros de configuração comuns.

O que se segue?

Você está pronto "configure o acesso aos dados"para de seus clientes SAN para o seu sistema ASA R2.

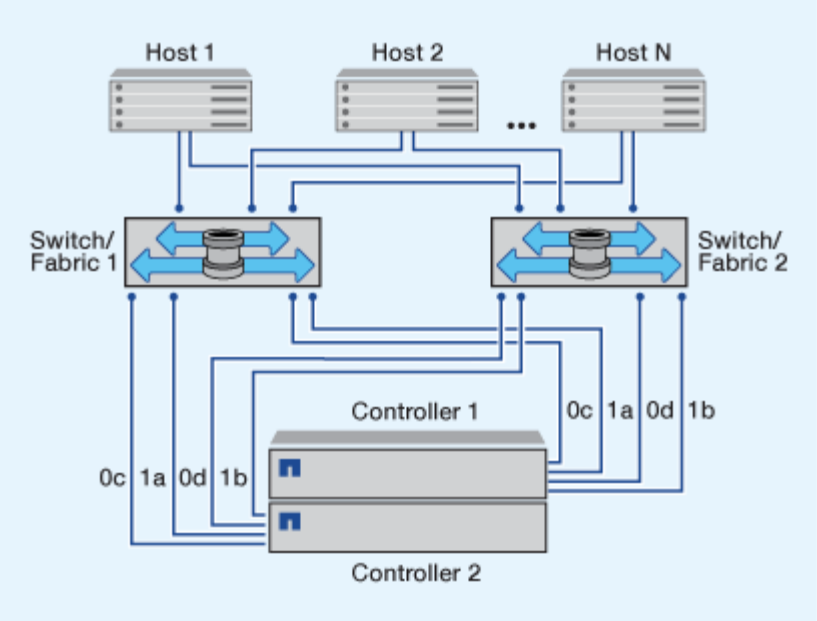
Configuração de host SAN com sistemas ASA R2

Os sistemas ASA R2 seguem as mesmas recomendações e diretrizes para a configuração de host SAN que todos os outros sistemas ONTAP.

É recomendável usar dois ou mais switches para conetar seu sistema de storage a um ou mais hosts SAN. Para configurações iSCSI, a topologia de rede que coneta seus hosts, switches e sistema de armazenamento é chamada de *network*. Para configurações FC e FC-NVMe, essa mesma topologia de rede é chamada de *Fabric*.

As configurações de várias malhas de várias redes (aquelas que usam dois ou mais switches) são recomendadas porque fornecem redundância tanto no switch quanto na camada de armazenamento. Essa redundância torna seu sistema de storage mais tolerante a falhas e oferece suporte a operações ininterruptas.

A ilustração a seguir é um exemplo de uma configuração FC com vários hosts usando duas fabrics para acessar um único par HA. Os números de porta de destino FC (0c, 0d, 1a, 1b) também são exemplos. Os números de porta reais variam dependendo do modelo do seu sistema e se você está usando adaptadores de expansão.



Saiba mais "Configuração SAN para hosts iSCSI"sobre o . Saiba mais "Configuração DE SAN para hosts FC e FC/NVMe"sobre o .

Recomendação de zoneamento para hosts FC

Você deve configurar seus hosts FC para usar o zoneamento. Os sistemas ASA R2 seguem as mesmas recomendações e diretrizes de zoneamento de host FC que todos os outros sistemas ONTAP.

Uma zona é um agrupamento lógico de uma ou mais portas dentro de uma malha. Para que os dispositivos possam se descobrir, estabelecer sessões umas com as outras e se comunicar, ambas as portas precisam ter uma associação de zona comum.

Saiba mais "Zoneamento FC/FC-NVMe"sobre o .

Habilite o acesso a dados de hosts SAN ao seu sistema de storage ASA R2

Para configurar o acesso aos dados, você deve garantir que os parâmetros críticos e as configurações do seu cliente SAN para operação adequada com o ONTAP estejam configurados corretamente. Se você estiver fornecendo armazenamento para o seu ambiente VMware, instale o OTV 10,3 para simplesmente o gerenciamento do armazenamento do ASA R2.

Configurar o acesso a dados a partir de hosts SAN

A configuração necessária para configurar o acesso de dados ao seu sistema ASA R2 a partir de seus hosts SAN varia dependendo do sistema operacional do host e do protocolo. A configuração correta é importante para o melhor desempenho e o failover bem-sucedido.

Consulte a documentação do host SAN ONTAP para "Clientes SCSI do VMware vSphere" "Clientes NVMe do VMware vSphere"e "Outros clientes SAN" para configurar corretamente os hosts para se conetar ao sistema ASA R2.

Migrar máquinas virtuais VMware

Se você precisar migrar sua carga de trabalho de VM de um sistema de armazenamento ASA para um sistema de armazenamento ASA r2, a NetApp recomenda que você use"VMware vSphere vMotion" para realizar uma migração ao vivo e sem interrupções dos seus dados.

As unidades de armazenamento ASA r2 são provisionadas dinamicamente por padrão. Ao migrar sua carga de trabalho de máquinas virtuais, os discos virtuais (VMDKs) também devem ser provisionados dinamicamente.

Informações relacionadas

- Saiba mais sobre "as vantagens de usar ONTAP para vSphere" .
- Aprenda sobre"Recuperação de site VMware Live com ONTAP" .
- Aprenda sobre"soluções de disponibilidade contínua para ambientes vSphere" .
- Saiba mais sobre"Como configurar o Broadcom VMware ESXi iSCSI MPIO com sistemas de armazenamento ONTAP SAN ASA" .

Migrar dados de um sistema de armazenamento de terceiros

A partir do ONTAP 9.17.1, você pode usar a Importação de LUN Estrangeiro (FLI) para migrar dados de um LUN em um sistema de armazenamento de terceiros para um sistema ASA r2. Usar a FLI para a migração de dados pode ajudar a reduzir o risco de perda de dados e tempo de inatividade durante o processo de migração.

O FLI oferece suporte a migrações online e offline. Em uma migração online, o sistema cliente permanece online enquanto os dados são copiados do sistema de armazenamento de terceiros para o sistema de armazenamento ONTAP . As migrações online são suportadas pelos sistemas operacionais host Windows, Linux e ESXi. Em uma migração offline, o sistema cliente é colocado offline, os dados da LUN são copiados do sistema de armazenamento de terceiros para o sistema de armazenamento ONTAP e, em seguida, o sistema cliente é reativado.

- Aprenda a realizar uma "Migração offline FLI" .
- Aprenda a realizar uma "Migrações online FLI" .

Configure o sistema ASA R2 como um fornecedor de storage no ambiente VMware

Você pode usar as ferramentas do ONTAP para VMware para habilitar facilmente o sistema ASA R2 como fornecedor de storage no ambiente VMware.

O ONTAP Tools for VMware vSphere é um conjunto de ferramentas que funcionam em conjunto com o VMware vCenter Server Virtual Appliance (vCSA) para facilitar o gerenciamento de máquinas virtuais em seus hosts VMware ESXi.

Os sistemas ASA R2 são suportados pela "Ferramentas do ONTAP para VMware vSphere 10,3" e posteriores.

Saiba como "Implantar as ferramentas do ONTAP para VMware"e, em seguida, use-o para fazer o seguinte:

- "Adicione instâncias do vCenter Server"
- "Configure as configurações do host ESXi"
- "Descubra os hosts e o sistema de storage do ASA R2"

O que se segue?

Você está pronto "provisionamento de storage"para permitir que seus hosts SAN leiam e gravem dados em unidades de storage.

Use o ONTAP para gerenciar seus dados

Demonstrações de vídeo do sistema de storage ASA R2

Veja vídeos curtos que demonstram como usar o Gerenciador de sistemas do ONTAP para executar tarefas comuns de forma rápida e fácil em seus sistemas de storage ASA R2.

Configure protocolos SAN no sistema ASA R2

"Transcrição de vídeo"

Provisione storage SAN em seu sistema ASA R2

"Transcrição de vídeo"

Replique dados para um cluster remoto a partir de um sistema ASA R2

"Transcrição de vídeo"

Gerencie seu storage

Provisione storage SAN ONTAP nos sistemas ASA R2

Quando você provisiona o storage, permite que seus hosts SAN leiam e gravem dados nos sistemas de storage ASA R2. Para provisionar o armazenamento, use o Gerenciador do sistema do ONTAP para criar unidades de armazenamento, adicionar iniciadores de host e mapear o host para uma unidade de armazenamento. Você também precisa executar etapas no host para ativar as operações de leitura/gravação.

Crie unidades de armazenamento

Em um sistema ASA r2, uma unidade de armazenamento disponibiliza espaço de armazenamento para os hosts SAN realizarem operações de dados. Uma unidade de armazenamento refere-se a um LUN para hosts SCSI ou a um namespace NVMe para hosts NVMe. Se o seu cluster estiver configurado para suportar hosts SCSI, você será solicitado a criar um LUN. Se o seu cluster estiver configurado para suportar hosts NVMe, você será solicitado a criar um namespace NVMe.

Uma unidade de armazenamento ASA r2 tem uma capacidade máxima de 128 TB. Veja o"NetApp Hardware Universe" Para obter as informações mais recentes sobre os limites de armazenamento para sistemas ASA r2.

Você adiciona e mapeia iniciadores de host para a unidade de armazenamento como parte do processo de criação da unidade de armazenamento. Você também pode"adicionar" e"mapa" Os iniciadores do host são criados após a criação das unidades de armazenamento.

A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots e habilitar a exclusão automática de snapshots ao criar uma unidade de armazenamento. A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots.

"Saiba mais sobre a reserva de snapshots em sistemas ASA r2.".

As unidades de armazenamento são provisionadas dinamicamente por padrão. O provisionamento dinâmico permite que a unidade de armazenamento cresça até o tamanho alocado, mas não reserva o espaço antecipadamente. O espaço é alocado dinamicamente a partir do espaço livre disponível, conforme a necessidade. Isso permite que você obtenha maior eficiência de armazenamento ao *provisionar em excesso* o espaço disponível. Por exemplo, suponha que você tenha 1 TB de espaço livre e precise criar quatro unidades de armazenamento de 1 TB. Em vez de adicionar imediatamente 3 TB de capacidade de armazenamento adicional ao seu sistema, você pode criar as unidades de armazenamento, monitorar a utilização do espaço e aumentar sua capacidade de armazenamento à medida que as unidades de armazenamento consomem espaço real. Saiba mais sobre"provisionamento fino" .

Passos

1. No System Manager, selecione **Storage** (armazenamento) e, em seguida, + Add selecione .
2. Introduza um nome para a nova unidade de armazenamento.
3. Introduza o número de unidades que pretende criar.

   Se você criar mais de uma unidade de armazenamento, cada unidade será criada com a mesma capacidade, sistema operacional host e mapeamento de host.

   Para otimizar o balanceamento da carga de trabalho em toda a zona de disponibilidade de armazenamento, crie um número par de unidades de armazenamento.

4. Introduza a capacidade da unidade de armazenamento e, em seguida, selecione o sistema operativo anfitrião.

   Se você estiver criando mais de uma unidade de armazenamento, cada unidade será criada com a mesma capacidade. Multiplique o número de unidades de armazenamento que você está criando pela capacidade desejada para garantir que tenha espaço útil suficiente. Se você não tiver espaço livre suficiente e optar por provisionar em excesso, monitore a utilização atentamente para evitar ficar sem espaço e perder dados.

5. Aceite o **mapeamento de host** selecionado automaticamente ou selecione um grupo de host diferente para a unidade de armazenamento a ser mapeada.

   Mapeamento de host refere-se ao grupo de hosts ao qual a nova unidade de armazenamento será mapeada. Se houver um grupo de hosts preexistente para o tipo de host selecionado para sua nova unidade de armazenamento, o grupo de hosts preexistente será selecionado automaticamente para seu mapeamento de hosts. Você pode aceitar o grupo de hosts selecionado automaticamente ou pode selecionar um grupo de hosts diferente.

   Se não existir um grupo de hosts pré-existente para hosts em execução no sistema operacional especificado, o ONTAP criará um novo grupo de hosts automaticamente.

6. Se você quiser fazer qualquer uma das seguintes opções, selecione **mais opções** e conclua as etapas necessárias.

Opção	Passos
Altere a política de qualidade do serviço (QoS) padrão Se a política de QoS padrão não tiver sido definida anteriormente na máquina virtual de armazenamento (VM) na qual a unidade de armazenamento está sendo criada, essa opção não estará disponível.	a. Em **armazenamento e otimização**, ao lado de **qualidade do serviço (QoS)**, selecione . b. Selecione uma política de QoS existente.
Crie uma nova política de QoS	a. Em **armazenamento e otimização**, ao lado de **qualidade do serviço (QoS)**, selecione . b. Selecione **Definir nova política**. c. Introduza um nome para a nova política de QoS. d. Defina um limite de QoS, uma garantia de QoS ou ambos. i. Opcionalmente, em **limit**, insira um limite máximo de throughput, um limite máximo de IOPS ou ambos. A configuração de uma taxa de transferência máxima e de IOPS para uma unidade de storage restringe o impacto nos recursos do sistema, de modo que não prejudique o desempenho de workloads críticos. ii. Opcionalmente, em **Guarantee**, insira uma taxa de transferência mínima, um mínimo de IOPS ou ambos. Definir uma taxa de transferência mínima e IOPS para uma unidade de storage garante que ela atenda aos requisitos mínimos de desempenho, independentemente da demanda por workloads da concorrência. e. Selecione **Adicionar**.
Altere o nível de serviço de desempenho padrão.	a. Em **armazenamento e otimização**, ao lado do **nível de serviço de desempenho**, selecione . b. Selecione **desempenho**. Os sistemas ASA r2 oferecem dois níveis de desempenho. O nível de desempenho padrão é **Extremo**, que é o nível mais alto disponível. Você pode diminuir o nível para **Desempenho**.
Modifique a reserva de snapshots padrão e habilite a exclusão automática de snapshots.	a. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots. b. Selecione **Excluir automaticamente snapshots antigos**.

Opção	Passos
Adicione um novo host SCSI	a. Em **informações do host**, selecione **SCSI** para o protocolo de conexão. b. Selecione o sistema operacional do host. c. Em **Mapeamento do host**, selecione **novos hosts**. d. Selecione **FC** ou **iSCSI**. e. Selecione iniciadores de host existentes ou selecione **Adicionar iniciador** para adicionar um novo iniciador de host. Um exemplo de uma WWPN FC válida é "01:02:03:04:0a:0b:0C:0d". Exemplos de nomes de iniciadores iSCSI válidos são "iqn.1995-08.com.example:string" e "eui.0123456789abcdef".
Crie um novo grupo de hosts SCSI	a. Em **informações do host**, selecione **SCSI** para o protocolo de conexão. b. Selecione o sistema operacional do host. c. Em **Mapeamento do host**, selecione **novo grupo de hosts**. d. Introduza um nome para o grupo anfitrião e, em seguida, selecione os anfitriões a adicionar ao grupo.
Adicionar um novo subsistema NVMe	a. Em **informações do host**, selecione **NVMe** para o protocolo de conexão. b. Selecione o sistema operacional do host. c. Em **Mapeamento do host**, selecione **novo subsistema NVMe**. d. Introduza um nome para o subsistema ou aceite o nome predefinido. e. Introduza um nome para o iniciador. f. Se pretender ativar a autenticação na banda ou a TLS (Transport Layer Security), selecione e, em seguida, selecione as suas opções. A autenticação na banda permite autenticação bidirecional e unidirecional segura entre os hosts NVMe e o sistema ASA R2. O TLS criptografa todos os dados enviados pela rede entre seus hosts NVMe/TCP e seu sistema ASA R2. g. Selecione **Adicionar iniciador** para adicionar mais iniciadores. Formate o NQN do host como <nqn.yyyy-mm> seguido por um nome de domínio totalmente qualificado. O ano deve ser igual ou posterior a 1970. O comprimento máximo total deve ser 223. Um exemplo de um iniciador NVMe válido é nqn.2014-08.com.example:string

7. Selecione **Adicionar**.

O que se segue?

Suas unidades de storage são criadas e mapeadas para seus hosts. Agora você pode "criar instantâneos"proteger os dados no seu sistema ASA R2.

Para mais informações

Saiba mais "Como os sistemas ASA R2 usam máquinas virtuais de armazenamento"sobre o .

Adicione iniciadores de host

Você pode adicionar novos iniciadores de host ao seu sistema ASA R2 a qualquer momento. Os iniciadores tornam os hosts elegíveis para acessar unidades de armazenamento e executar operações de dados.

Antes de começar

Se você quiser replicar a configuração do host para um cluster de destino durante o processo de adição de iniciadores de host, o cluster deve estar em um relacionamento de replicação. Opcionalmente, você pode "crie uma relação de replicação" depois que seu host for adicionado.

Adicione iniciadores de host para hosts SCSI ou NVMe.

SCSI anfitriões

Passos

1. Selecione **Host**.
2. Selecione **SCSI**; em seguida, + Add selecione .
3. Digite o nome do host, selecione o sistema operacional do host e insira uma descrição do host.
4. Se você quiser replicar a configuração do host para um cluster de destino, selecione **replique a configuração do host** e, em seguida, selecione o cluster de destino.

   O cluster precisa estar em uma relação de replicação para replicar a configuração do host.

5. Adicione hosts novos ou existentes.

Adicione novos hosts	Adicionar hosts existentes
a. Selecione **novos hosts**. b. Selecione **FC** ou **iSCSI**; em seguida, selecione os iniciadores do host. c. Opcionalmente, selecione **Configurar proximidade do host**. A configuração da proximidade do host permite que o ONTAP identifique a controladora mais próxima do host para otimização do caminho de dados e redução da latência. Isso só se aplica se você tiver replicado dados para um local remoto. Se não tiver configurado a replicação de instantâneos, não será necessário selecionar esta opção. d. Se precisar adicionar novos iniciadores, selecione **Adicionar iniciadores**.	a. Selecione **hosts existentes**. b. Selecione o host que você deseja adicionar. c. Selecione **Adicionar**.

6. Selecione **Adicionar**.

O que se segue?

Seus hosts SCSI são adicionados ao seu sistema ASA R2 e você está pronto para mapear seus hosts para suas unidades de armazenamento.

Hosts NVMe

Passos

1. Selecione **Host**.
2. Selecione **NVMe**; em seguida, + Add selecione .
3. Insira um nome para o subsistema NVMe, selecione o sistema operacional host e insira uma descrição.
4. Selecione **Adicionar iniciador**.

O que se segue?

Seus hosts NVMe são adicionados ao sistema ASA R2 e você está pronto para mapear seus hosts para suas unidades de storage.

Mapear a unidade de armazenamento para um host

Após criar as unidades de armazenamento ASA r2 e adicionar os iniciadores de host, mapeie os hosts para as unidades de armazenamento para começar a fornecer dados. As unidades de armazenamento são mapeadas para os hosts como parte do processo de criação da unidade de armazenamento. Você também pode mapear unidades de armazenamento existentes para hosts novos ou existentes a qualquer momento.

Passos

1. Selecione **armazenamento**.
2. Passe o cursor sobre o nome da unidade de armazenamento que pretende mapear.
3. Selecione ⋮ ; em seguida, selecione **Map to hosts**.
4. Selecione os hosts que deseja mapear para a unidade de armazenamento; em seguida, selecione **Map**.

O que se segue?

Sua unidade de armazenamento é mapeada para seus hosts e você está pronto para concluir o processo de provisionamento em seus hosts.

Provisionamento completo no lado do host

Depois de criar suas unidades de armazenamento, adicionar seus iniciadores de host e mapear suas unidades de armazenamento, há etapas que você deve executar em seus hosts antes que eles possam ler e gravar dados em seu sistema ASA R2.

Passos

1. Para FC e FC/NVMe, defina a zona dos switches FC por WWPN.

   Use uma zona por iniciador e inclua todas as portas de destino em cada zona.

2. Descubra a nova unidade de armazenamento.
3. Inicialize a unidade de armazenamento e um sistema de criação de ficheiros.
4. Verifique se o host pode ler e gravar dados na unidade de armazenamento.

O que se segue?

Você concluiu o processo de provisionamento e está pronto para começar a fornecer dados. Agora você pode "criar instantâneos"proteger os dados no seu sistema ASA R2.

Para mais informações

Para obter mais detalhes sobre a configuração do lado do host, consulte "Documentação do host SAN ONTAP"o para seu host específico.

Clonar dados em sistemas de storage ASA R2

A clonagem de dados cria cópias de unidades de storage e grupos de consistência no sistema ASA R2 usando o Gerenciador de sistemas do ONTAP que pode ser usado para desenvolvimento de aplicações, testes, backups, migração de dados ou outras funções administrativas.

Clonar unidades de storage

Ao clonar uma unidade de storage, você cria uma nova unidade de storage no sistema ASA R2 que é uma cópia gravável e pontual da unidade de storage clonada.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja clonar.
3. Selecione ⋮ ; em seguida, selecione **Clone**.
4. Aceite o nome padrão para a nova unidade de armazenamento que será criada como um clone ou insira um novo.
5. Selecione o sistema operacional do host.

   Um novo snapshot é criado para o clone por padrão.

6. Se você quiser usar um snapshot existente, criar um novo grupo de hosts ou adicionar um novo host, selecione **mais opções**.

Opção	Passos
Use um instantâneo existente	a. Em **Snapshot to clone**, selecione **Use an existing snaphot**. b. Selecione o instantâneo que deseja usar para o clone.
Crie um novo grupo de hosts	a. Em **Host mapping**, selecione **New host group**. b. Insira um nome para o novo grupo de hosts; em seguida, selecione os iniciadores de host a serem incluídos no grupo.
Adicione um novo host	a. Em **Host mapping**, selecione **New hosts**. b. Insira o nome a para o novo host; em seguida, selecione **FC** ou **iSCSI**. c. Selecione os iniciadores do host na lista de iniciadores existentes ou selecione **Adicionar** para adicionar novos iniciadores para o host.

7. Selecione **Clone**.

O que se segue?

Criou uma nova unidade de armazenamento idêntica à unidade de armazenamento clonada. Agora está pronto para utilizar a nova unidade de armazenamento, conforme necessário.

Grupos de consistência de clones

Ao clonar um grupo de consistência, você cria um novo grupo de consistência idêntico à estrutura, às unidades de storage e aos dados do grupo de consistência clonado. Use um clone de grupo de consistência para realizar testes de aplicações ou migrar dados. Suponha, por exemplo, que você precise migrar uma carga de trabalho de produção de um grupo de consistência. Você pode clonar o grupo de consistência para

criar uma cópia do workload de produção e mantê-lo como um backup até que a migração seja concluída.

O clone é criado a partir de um snapshot do grupo de consistência que está sendo clonado. O snapshot usado para o clone é feito no momento em que o processo de clonagem é iniciado por padrão. Você pode modificar o comportamento padrão para usar um instantâneo pré-existente.

Mapeamentos de unidades de armazenamento são copiados como parte do processo de clonagem. As políticas de snapshot não são copiadas como parte do processo de clonagem.

É possível criar clones de grupos de consistência armazenados localmente no sistema ASA R2 ou de grupos de consistência replicados para locais remotos.

Clone usando snapshot local

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja clonar.
3. Selecione e, em seguida, selecione **Clone**.
4. Insira um nome para o clone do grupo de consistência ou aceite o nome padrão.
5. Selecione o sistema operacional do host.
6. Se você quiser dissociar o clone do grupo de consistência de origem e alocar espaço em disco, selecione **Split clone**.
7. Se você quiser usar um snapshot existente, criar um novo grupo de hosts ou adicionar um novo host para o clone, selecione **mais opções**.

Opção	Passos
Use um instantâneo existente	a. Em **Snapshot to clone**, selecione **Use an existing snapshot**. b. Selecione o instantâneo que deseja usar para o clone.
Crie um novo grupo de hosts	a. Em **Host mapping**, selecione **New host group**. b. Insira um nome para o novo grupo de hosts; em seguida, selecione os iniciadores de host a serem incluídos no grupo.
Adicione um novo host	a. Em **Host mapping**, selecione **New hosts**. b. Introduza o nome do novo nome de anfitrião; em seguida, selecione **FC** ou **iSCSI**. c. Selecione os iniciadores do host na lista de iniciadores existentes ou selecione **Adicionar iniciador** para adicionar novos iniciadores para o host.

8. Selecione **Clone**.

Clone usando snapshot remoto

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Passe o Mouse sobre o **Source** que você deseja clonar.
3. Selecione e, em seguida, selecione **Clone**.
4. Selecione o cluster de origem e a VM de armazenamento; em seguida, introduza um nome para o novo grupo de consistência ou aceite o nome predefinido.
5. Selecione o instantâneo para clonar; em seguida, selecione **Clone**.

O que se segue?

Clonou um grupo de consistência a partir da sua localização remota. O novo grupo de consistência está disponível localmente no seu sistema ASA R2 para ser usado conforme necessário.

O que se segue?

Para proteger seus dados, você deve "criar instantâneos"do grupo de consistência clonada.

Clone de grupo de consistência dividida

Quando você divide um clone de grupo de consistência, dissocia o clone do grupo de consistência de origem e aloca espaço em disco para o clone. O clone se torna um grupo de consistência autônomo que pode ser usado independentemente do grupo de consistência de origem.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o clone do grupo de consistência que você deseja dividir.
3. Selecione **Split clone**.
4. Selecione **Split**.

Resultado

O clone é dissociado do grupo de consistência de origem e o espaço em disco é alocado para o clone.

Gerenciar grupos de hosts

Crie grupos de hosts no seu sistema ASA r2

Em um sistema ASA R2, um *grupo de hosts* é o mecanismo usado para dar aos hosts acesso a unidades de armazenamento. Um grupo de hosts se refere a um iggroup para hosts SCSI ou a um subsistema NVMe para hosts NVMe. Um host só pode ver as unidades de armazenamento mapeadas para os grupos de hosts aos quais pertence. Quando um grupo de hosts é mapeado para uma unidade de armazenamento, os hosts que são membros do grupo são então capazes de montar (criar diretórios e estruturas de arquivo) a unidade de armazenamento.

Os grupos de hosts são criados automaticamente ou manualmente quando você cria suas unidades de storage. Opcionalmente, você pode usar as etapas a seguir para criar grupos de hosts antes ou depois da criação da unidade de armazenamento.

Passos

1. No System Manager, selecione **Host**.
2. Selecione os hosts que você deseja adicionar ao grupo de hosts.

   Depois de selecionar o primeiro host, a opção para adicionar a um grupo de hosts aparece acima da lista de hosts.

3. Selecione **Adicionar ao grupo anfitrião**.
4. PESQUISE e selecione o grupo de hosts ao qual você deseja adicionar o host.

O que se segue?

Você criou um grupo de hosts e agora pode "mapeie-o para uma unidade de armazenamento" .

Excluir um grupo de hosts no seu sistema ASA r2

Em um sistema ASA r2, um grupo de hosts é o mecanismo usado para conceder aos hosts acesso às unidades de armazenamento. Um grupo de hosts refere-se a um igroup para hosts SCSI ou a um subsistema NVMe para hosts NVMe. Um host só pode ver as unidades de armazenamento mapeadas aos grupos de hosts aos quais pertence. Talvez você queira excluir um grupo de hosts se não quiser mais que os hosts do grupo tenham acesso às unidades de armazenamento mapeadas a ele.

Passos

1. No System Manager, selecione **Storage**.
2. Em **Mapeamento de host**, selecione o grupo de hosts que você deseja excluir.
3. Selecione **Armazenamento mapeado**.
4. Selecione **Mais**; depois selecione **Excluir**.
5. Selecione para verificar se você deseja continuar; depois selecione **Excluir**.

O que se segue?

O grupo de hosts é excluído. Os hosts que estavam no grupo não têm mais acesso às unidades de armazenamento mapeadas para o grupo de hosts.

Gerenciar unidades de armazenamento

Modificar unidades de storage em sistemas de storage ASA R2

Para otimizar a performance do seu sistema ASA R2, talvez seja necessário modificar as unidades de storage para aumentar a capacidade, atualizar políticas de QoS ou alterar os hosts mapeados para as unidades. Por exemplo, se um novo workload de aplicativo crítico for adicionado a uma unidade de storage existente, talvez seja necessário alterar a política de qualidade do serviço (QoS) aplicada à unidade de storage para dar suporte ao nível de performance necessário para o novo aplicativo.

Aumentar a capacidade

Aumente o tamanho de uma unidade de armazenamento antes de atingir a capacidade máxima para evitar a perda de acesso aos dados que pode ocorrer se a unidade de armazenamento ficar sem espaço gravável. A capacidade de uma unidade de armazenamento pode ser aumentada para 128 TB, que é o tamanho máximo permitido pela ONTAP.

Modifique mapeamentos de host

Modifique os hosts mapeados para uma unidade de storage para auxiliar no balanceamento de cargas de trabalho ou na reconfiguração de recursos do sistema.

Modificar política de QoS

As políticas de qualidade do serviço (QoS) garantem que a performance de workloads essenciais não seja degradada pelos workloads da concorrência. Você pode usar políticas de QoS para definir uma taxa de transferência de QoS *limit* e uma taxa de transferência de QoS *guarantee*.

- Limite de taxa de transferência de QoS

  A taxa de transferência de QoS *limit* restringe o impacto de um workload nos recursos do sistema, limitando a taxa de transferência do workload a um número máximo de IOPS ou Mbps, ou IOPS e Mbps.

- Garantia de taxa de transferência de QoS

  A taxa de transferência de QoS *guarantee* garante que workloads críticos atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workloads da concorrência, garantindo que a taxa de transferência para o workload crítico não fique abaixo de um número mínimo de IOPS ou Mbps, ou IOPS e Mbps.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja editar.
3. Selecione ⋮; em seguida, selecione **Editar**.
4. Atualize os parâmetros da unidade de armazenamento conforme necessário para aumentar a capacidade, alterar a política de QoS e atualizar o mapeamento do host.

O que se segue?

Se tiver aumentado o tamanho da sua unidade de armazenamento, tem de voltar a digitalizar a unidade de armazenamento no anfitrião para que o anfitrião reconheça a alteração de tamanho.

Mova unidades de storage nos sistemas de storage ASA R2

Se uma zona de disponibilidade de storage estiver com pouco espaço, você poderá mover unidades de armazenamento para outra zona de disponibilidade de armazenamento para equilibrar a utilização de armazenamento no cluster.

Você pode mover uma unidade de armazenamento enquanto a unidade de armazenamento está on-line e fornecendo dados. A operação de movimentação não causa interrupções.

Antes de começar

- Você deve estar executando o ONTAP 9.16,1 ou posterior.
- O cluster precisa ser composto por quatro ou mais nós.

Passos

1. No System Manager, selecione **Storage** (armazenamento) e, em seguida, selecione a unidade de armazenamento que pretende mover.
2. Selecione ⋮; em seguida, selecione **mover**.
3. Selecione a zona de disponibilidade de armazenamento para a qual pretende mover a unidade de armazenamento; em seguida, selecione **mover**.

Excluir unidades de armazenamento em sistemas de armazenamento ASA R2

Elimine uma unidade de armazenamento se já não necessitar de manter os dados contidos na unidade. A exclusão de unidades de armazenamento que não são mais necessárias pode ajudá-lo a liberar espaço necessário para outros aplicativos host.

Antes de começar

Se a unidade de armazenamento que você deseja excluir estiver em um grupo de consistência que esteja em um relacionamento de replicação, você deverá"retire a unidade de armazenamento do grupo de consistência" antes de excluí-lo.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja excluir.
3. Selecione ; em seguida, selecione **Delete**.
4. Reconheça que a exclusão não pode ser desfeita.
5. Selecione **Eliminar**.

O que se segue?

Você pode usar o espaço liberado da unidade de armazenamento excluída para "aumente o tamanho"unidades de armazenamento que precisam de capacidade adicional.

Migrar VMs de armazenamento

Migrar uma VM de armazenamento de um cluster ASA para um cluster ASA R2.

A partir do ONTAP 9.18.1, você pode migrar uma máquina virtual (VM) de armazenamento de qualquer cluster ASA para qualquer cluster ASA R2 sem interrupções. A migração de um cluster ASA para um cluster ASA r2 permite adotar a arquitetura simplificada e otimizada dos sistemas ASA r2 para ambientes exclusivamente SAN.

A migração de máquinas virtuais de armazenamento entre sistemas de armazenamento ASA e ASA R2 é suportada da seguinte forma:

De qualquer um dos seguintes sistemas ASA :	Para qualquer um dos seguintes sistemas ASA r2:
• ASA C800 • ASA C400 • ASA C250 • ASA A900 • ASA A800 • ASA A400 • ASA A250 • ASA A150 • ASA AFF A800 • ASA AFF A700 • ASA AFF A400 • ASA AFF A250 • ASA AFF A220	• ASA A1K • ASA C30 • ASA A90 • ASA A70 • ASA A50 • ASA A30 • ASA A20

Para obter a lista mais atualizada de sistemas ASA e ASA r2, consulte"NetApp Hardware Universe" . Os sistemas ASA r2 estão listados no NetApp Hardware Universe como "ASA Série A/Série C (Novo)".

Você só pode migrar uma VM de armazenamento para um cluster ASA r2 a partir de um cluster ASA . A migração de qualquer outro tipo de sistema ONTAP não é suportada.

Antes de começar

Todos os nós do cluster ASA r2 e o próprio cluster ASA devem estar executando o ONTAP 9.18.1 ou posterior. As versões de patch do ONTAP 9.18.1 nos nós do cluster podem variar.

Etapa 1: Verifique o status da VM de armazenamento ASA

Antes de migrar uma VM de armazenamento de um sistema ASA , não deve haver namespaces NVMe ou vVols presentes, e cada volume na VM de armazenamento deve conter apenas um LUN. A migração de namespaces NVMe e vVols não é suportada. A arquitetura dos sistemas ASA r2 exige que os volumes contenham um único LUN.

Passos

1. Verifique se não há namespaces NVMe presentes na máquina virtual de armazenamento:

   ```
   vserver nvme namespace show -vserver <storage_VM>
   ```

   Se as entradas forem exibidas, os objetos NVMe devem ser"convertido" para LUNs ou removidos. Veja o `vserver nvme namespace delete` e o `vserver nvme subsystem delete` comandos no"Referência do comando ONTAP" Para obter mais informações.

2. Verifique se não há vVols presentes na VM de armazenamento:

   ```
   lun show -verser <storage_VM> -class protocol-endpoint,vvol
   ```

   Caso existam vVols , eles devem ser copiados para outra VM de armazenamento e, em seguida, excluídos da VM de armazenamento a ser migrada. Veja o `lun copy` e `lun delete` comandos no"Referência do comando ONTAP" Para obter mais informações.

3. Verifique se cada volume na máquina virtual de armazenamento contém um único LUN:

   ```
   lun show -verser <storage_VM>
   ```

   Se um volume contiver mais de um LUN, use o `volume create` e `lun move` comandos para criar uma relação de volume para LUN de 1:1. Veja o"Referência do comando ONTAP" para mais informações.

O que vem a seguir?

Você está pronto para criar uma relação de pares de cluster entre seus clusters ASA e ASA R2.

Etapa 2: Crie uma relação de pares de cluster entre seus clusters ASA e ASA R2.

Antes de migrar uma VM de armazenamento de um cluster ASA para um cluster ASA R2, você precisa criar uma relação de pares. Uma relação ponto a ponto define conexões de rede que permitem que clusters ONTAP e máquinas virtuais de armazenamento troquem dados com segurança.

Antes de começar

Você deve ter criado LIFs intercluster em todos os nós dos clusters que estão sendo interligados, usando um dos seguintes métodos.

- "Configure LIFs intercluster em portas de dados compartilhadas."
- "Configure LIFs intercluster em portas de dados dedicadas."
- "Configure LIFs entre clusters em espaços IP personalizados."

Passos

1. No cluster ASA r2, crie uma relação de pares com o cluster ASA e gere uma senha:

   ```
   cluster peer create -peer-addrs <ASA_cluster_LIF_IPs> -generate
   -passphrase
   ```

   O exemplo a seguir cria uma relação de pares entre o cluster 1 e o cluster 2 e gera uma senha automática pelo sistema:

   ```
   cluster1::> cluster peer create -peer-addrs 10.98.191.193 -generate
   -passphrase
   Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Peer Cluster Name: cluster2
               Initial Allowed Vserver Peers: -
               Expiration Time: 6/7/2017 09:16:10 +5:30
               Intercluster LIF IP: 10.140.106.185
   Warning: make a note of the passphrase - it cannot be displayed again.
   ```

2. Copie a senha gerada.
3. No cluster ASA , crie uma relação de pares com o cluster ASA r2:

   ```
   cluster peer create -peer-addrs <ASA_r2_LIF_IPs>
   ```

4. Digite a senha gerada no cluster ASA r2.
5. Verifique se a relação de pares do cluster foi criada:

   ```
   cluster peer show
   ```

   O exemplo a seguir exibe a saída esperada para clusters emparelhados com sucesso.

```
cluster1::> cluster peer show

Peer Cluster Name   Cluster Serial Number   Availability
Authentication
-----------------   ---------------------   --------------
--------------
cluster2             1-80-123456             Available      ok
```

Resultado

Os clusters ASA e ASA R2 estão interligados e os dados das máquinas virtuais de armazenamento podem ser transferidos com segurança.

O que vem a seguir?

Você está pronto para preparar sua VM de armazenamento ASA para migração.

Etapa 3: Prepare-se para a migração da VM de armazenamento de um cluster ASA para um cluster ASA R2.

Antes de migrar uma máquina virtual (VM) de armazenamento de um cluster ASA para um cluster ASA R2, você deve executar uma verificação prévia de migração e corrigir quaisquer problemas necessários. Não é possível realizar a migração até que a verificação prévia seja concluída com sucesso.

Passo

1. A partir do seu cluster ASA r2, execute a verificação prévia de migração:

   ```
   vserver migrate start -vserver <storage_VM> -source-cluster
   <asa_cluster> -check-only true
   ```

   Caso precise corrigir algum problema para preparar seu cluster ASA para migração, o problema e a ação corretiva serão exibidos. Corrija o problema e repita a verificação prévia até que ela seja concluída com sucesso.

O que vem a seguir?

Você está pronto para migrar sua VM de armazenamento do seu cluster ASA para um cluster ASA R2.

Etapa 4: Migrar uma VM de armazenamento ASA para um cluster ASA R2

Após preparar o cluster ASA e criar a relação de pares necessária com o cluster ASA R2, você pode iniciar a migração da VM de armazenamento.

Ao realizar uma migração de VM de armazenamento, é uma prática recomendada deixar 30% de folga na CPU tanto no cluster ASA quanto no cluster ASA R2 para permitir a execução da carga de trabalho da CPU.

Sobre esta tarefa

Após a migração da máquina virtual de armazenamento, os clientes são automaticamente transferidos para o cluster ASA r2 e a máquina virtual de armazenamento no cluster ASA é removida automaticamente. A migração automática e a remoção automática de máquinas virtuais de armazenamento estão ativadas por padrão. Opcionalmente, você pode desativá-los e realizar a migração e a remoção da máquina virtual de armazenamento manualmente.

Antes de começar

- O cluster ASA r2 deve ter espaço livre suficiente para acomodar a VM de armazenamento migrada.
- Se a máquina virtual de armazenamento do ASA contiver volumes criptografados, o gerenciador de chaves integrado ou o gerenciador de chaves externo no sistema ASA r2 deverá ser configurado no nível do cluster.
- As seguintes operações não podem ser executadas no cluster ASA de origem:
  - operações de failover
  - WAFLIRON
  - Impressão digital
  - Movimentação, rehospedagem, clonagem, criação, conversão ou análise de volume

Passos

1. A partir do cluster ASA r2, inicie a migração da VM de armazenamento:

   ```
   vserver migrate start -vserver <storage_VM_name> -source-cluster
   <ASA_cluster>
   ```

   Para desativar a transição automática, use o `-auto-cutover false` parâmetro. Para desativar a remoção automática da VM de armazenamento ASA , use o `-auto-source-cleanup false` parâmetro.

2. Acompanhe o andamento da migração.

   ```
   vserver migrate show -vserver <storage_VM_name>
   ```

   Quando a migração estiver concluída, o **status** será exibido como **migration-complete**.

> Se precisar pausar ou cancelar a migração antes do início da transição automática, use o `vserver migrate pause` e o `vserver migrate abort` comandos. Você deve pausar a migração antes de cancelá-la. Não é possível cancelar a migração após o início do processo de transição.

Resultado

A máquina virtual de armazenamento foi migrada do cluster ASA para o cluster ASA R2. O nome e o UUID da máquina virtual de armazenamento, o nome da LIF de dados, o endereço IP e os nomes dos objetos, como o nome do volume, permanecem inalterados. Os UUIDs dos objetos migrados na VM de armazenamento são atualizados.

O que vem a seguir?

Se você desativou a migração automática e a remoção automática de máquinas virtuais de armazenamento,"Migre manualmente seus clientes ASA para o cluster ASA R2 e remova a VM de armazenamento do cluster ASA." .

Migrar clientes e limpar a VM de armazenamento de origem após a migração para um sistema ASA r2.

Após uma máquina virtual (VM) de armazenamento ser migrada de um cluster ASA para

um cluster ASA R2, por padrão, os clientes são automaticamente transferidos para o cluster ASA R2 e a VM de armazenamento no cluster ASA é removida automaticamente. Se você optou por desativar a transferência e remoção automáticas da VM de armazenamento ASA durante a migração, será necessário executar essas etapas manualmente após a conclusão da migração.

Migrar manualmente os clientes para um sistema ASA r2 após a migração de uma máquina virtual de armazenamento.

Se você desativar a transição automática de clientes durante a migração de uma VM de armazenamento de um cluster ASA para um cluster ASA R2, após a conclusão bem-sucedida da migração, execute a transição manualmente para que a VM de armazenamento ASA R2 possa fornecer dados aos clientes.

Passos

1. No cluster ASA r2, execute manualmente a migração do cliente:

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. Verifique se a operação de transição foi concluída:

```
vserver migrate show
```

Resultado

Os dados estão sendo fornecidos aos seus clientes a partir da máquina virtual de armazenamento no seu cluster ASA r2.

O que vem a seguir?

Agora você está pronto para remover a VM de armazenamento do cluster ASA de origem.

Remover manualmente uma VM de armazenamento ASA após a migração para um cluster ASA R2

Se você desativar a limpeza automática da origem durante a migração de uma VM de armazenamento de um cluster ASA para um cluster ASA R2, após a conclusão da migração, remova a VM de armazenamento do cluster ASA para liberar espaço de armazenamento.

Antes de começar

Seus clientes devem estar fornecendo dados do cluster ASA r2.

Passos

1. No cluster ASA , verifique se o status da VM de armazenamento ASA é **Pronto para limpeza de origem**:

```
vserver migrate show
```

2. Remova a VM de armazenamento ASA :

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

Resultado

A máquina virtual de armazenamento no seu cluster ASA foi removida.

Limites de armazenamento do ASA R2

Para obter o melhor desempenho, configuração e suporte, você deve estar ciente dos limites de armazenamento do ASA r2.

Para obter uma lista completa dos limites de armazenamento mais atuais do ASA R2, "NetApp Hardware Universe"consulte .

Os sistemas ASA r2 suportam os seguintes limites de armazenamento:

	Máximo por par de HA	Máximo por grupo
Grupos de consistência	256	256
Aplicações empresariais	100	350
Nós	2	12
Grupos de replicação	50	50
Tamanho da zona de disponibilidade de armazenamento	2 PB	2 PB
Unidades de armazenamento	10.000	30.000
Tamanho da unidade de armazenamento	128 TB	128 TB
Unidades de armazenamento por grupo de consistência	256	256
Grupos de consistência infantil por grupo de consistência parental	64	64
Máquinas virtuais de armazenamento	• 256 (ONTAP 9.18.1 e posterior) • 32 (ONTAP 9.17.1 e versões anteriores)	• 256 (ONTAP 9.18.1 e posterior) • 32 (ONTAP 9.17.1 e versões anteriores)
Máquinas virtuais	800	1200

Limites para relacionamentos assíncronos do SnapMirror

Os limites a seguir se aplicam a unidades de armazenamento e grupos de consistência em um relacionamento de replicação assíncrona do SnapMirror . Para obter uma lista completa dos limites de armazenamento mais recentes do ASA r2,"NetApp Hardware Universe" .

Limite máximo	Por par de HA	Por cluster
Grupos de consistência	250	750
Unidades de armazenamento	4.000	6.000

Limites para relacionamento de sincronização ativa do SnapMirror

Os limites a seguir se aplicam a unidades de armazenamento e grupos de consistência em um relacionamento de replicação de sincronização ativa do SnapMirror . A sincronização ativa do SnapMirror é suportada a partir do ONTAP 9.17.1, somente em clusters de dois nós. A partir do ONTAP 9.18.1, a sincronização ativa do SnapMirror é suportada em clusters de quatro nós.

Para obter uma lista completa dos limites de armazenamento mais recentes do ASA r2,"NetApp Hardware Universe" .

Limite máximo	Por par de HA
Grupos de consistência	50
Unidades de armazenamento	400

Proteja seus dados

Crie snapshots para fazer backup de seus dados em sistemas de storage ASA R2

Crie um snapshot para fazer backup dos dados no seu sistema ASA r2. Utilize o ONTAP System Manager para criar um snapshot manual de uma única unidade de armazenamento ou para criar um grupo de consistência e agendar snapshots automáticos de várias unidades de armazenamento simultaneamente.

Passo 1: Opcionalmente, crie um grupo de consistência

Um grupo de consistência é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade. Crie grupos de consistência para simplificar o gerenciamento de storage e a proteção de dados para workloads de aplicações que abrangem várias unidades de storage. Por exemplo, suponha que você tenha um banco de dados composto por 10 unidades de armazenamento em um grupo de consistência, e você precisa fazer backup de todo o banco de dados. Em vez de fazer backup de cada unidade de armazenamento, você pode fazer backup de todo o banco de dados simplesmente adicionando proteção de dados snapshot ao grupo de consistência.

Crie um grupo de consistência usando novas unidades de armazenamento ou crie um grupo de consistência usando unidades de armazenamento existentes.

A partir do ONTAP 9.18.1, você pode definir a porcentagem de reserva de snapshots e habilitar a exclusão automática de snapshots ao criar um grupo de consistência com novas unidades de armazenamento. A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Se a reserva de snapshots e a exclusão automática de snapshots estiverem ativadas em um grupo de consistência pai, elas serão ativadas em todos os grupos de consistência filho existentes. Se novos grupos de consistência filhos forem adicionados, eles não herdarão as configurações de reserva e exclusão de instantâneos do grupo pai.

"Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2.".

A partir do ONTAP 9.16.1, ao criar grupos de consistência usando novas unidades de armazenamento, você pode configurar até cinco grupos de consistência filhos. "Saiba mais sobre grupos de consistência infantil em sistemas ASA r2".

Use novas unidades de armazenamento

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. + Add Selecione ; em seguida, selecione **usando novas unidades de armazenamento**.
3. Introduza um nome para a nova unidade de armazenamento, o número de unidades e a capacidade por unidade.

   Se você criar mais de uma unidade, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host por padrão. Opcionalmente, você pode atribuir uma capacidade diferente a cada unidade.

4. Se você quiser fazer qualquer uma das seguintes opções, selecione **mais opções** e conclua as etapas necessárias.

Opção	Passos
Atribua uma capacidade diferente a cada unidade de armazenamento	Selecione **Adicionar uma capacidade diferente**.
Altere o nível de serviço de desempenho padrão	Em **nível de serviço de desempenho**, selecione um nível de serviço diferente. Os sistemas ASA r2 oferecem dois níveis de desempenho. O nível de desempenho padrão é **Extremo**, que é o nível mais alto disponível. Você pode reduzir o nível de desempenho para **Desempenho**.
Modifique a reserva de snapshots padrão e habilite a exclusão automática de snapshots.	a. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots. b. Selecione **Excluir automaticamente snapshots antigos**.
Crie um grupo de consistência filho	Selecione **Adicionar grupo de consistência filho**.

5. Selecione o sistema operacional do host e o mapeamento do host.
6. Selecione **Adicionar**.

O que se segue?

Você criou um grupo de consistência contendo as unidades de armazenamento que deseja proteger. Agora você pode criar um instantâneo.

Use unidades de armazenamento existentes

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. + Add Selecione ; em seguida, selecione **usando unidades de armazenamento existentes**.

3. Introduza um nome para o grupo de consistência; em seguida, procure e selecione as unidades de armazenamento que pretende incluir no grupo de consistência.
4. Selecione **Adicionar**.

O que se segue?

Você criou um grupo de consistência contendo as unidades de armazenamento que deseja proteger. Agora você pode criar um instantâneo.

Passo 2: Crie um instantâneo

Um instantâneo é uma cópia local e somente leitura de seus dados que você pode usar para restaurar unidades de armazenamento em pontos específicos no tempo.

Os instantâneos podem ser criados sob demanda ou podem ser criados automaticamente em intervalos regulares com base em um "política e agendamento de snapshot". A política e a programação de snapshot especificam quando criar os snapshots, quantas cópias devem ser mantidas, como nomeá-los e como rotulá-los para replicação. Por exemplo, um sistema pode criar um snapshot todos os dias às 12:10 da manhã, reter as duas cópias mais recentes, nomeá-las "diariamente" (anexado com um carimbo de data/hora) e rotulá-las "diariamente" para replicação.

Tipos de instantâneos

Você pode criar um snapshot sob demanda de uma única unidade de armazenamento ou de um grupo de consistência. Você pode criar snapshots automatizados de um grupo de consistência que contém várias unidades de storage. Não é possível criar instantâneos automatizados de uma única unidade de armazenamento.

- Snapshots sob demanda

  Você pode criar um instantâneo sob demanda de uma unidade de armazenamento a qualquer momento. A unidade de armazenamento não precisa ser membro de um grupo de consistência para ser protegida por um snapshot sob demanda. Se você criar um snapshot sob demanda de uma unidade de armazenamento que seja membro de um grupo de consistência, as outras unidades de armazenamento no grupo de consistência não serão incluídas no snapshot sob demanda. Se você criar um instantâneo sob demanda de um grupo de consistência, todas as unidades de armazenamento do grupo de consistência serão incluídas no instantâneo.

- Snapshots automatizados

  Snapshots automatizados são criados usando políticas de snapshot. Para aplicar uma política de instantâneos a uma unidade de armazenamento para criação automática de instantâneos, a unidade de armazenamento deve ser membro de um grupo de consistência. Se você aplicar uma política de snapshot a um grupo de consistência, todas as unidades de storage do grupo de consistência serão protegidas com snapshots automatizados.

Crie um instantâneo de um grupo de consistência ou de uma unidade de armazenamento.

Instantâneo de um grupo de consistência

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o nome do grupo de consistência que você deseja proteger.
3. Selecione ⋮ ; em seguida, selecione **proteger**.
4. Se você quiser criar um instantâneo imediato sob demanda, em **proteção local**, selecione **Adicionar um instantâneo agora**.

   A proteção local cria o instantâneo no mesmo cluster que contém a unidade de armazenamento.

   a. Insira um nome para o instantâneo ou aceite o nome padrão; em seguida, opcionalmente, insira um rótulo SnapMirror.

      A etiqueta SnapMirror é utilizada pelo destino remoto.

5. Se você quiser criar snapshots automatizados usando uma política de snapshot, selecione **Agendar snapshots**.

   a. Selecione uma política de instantâneos.

      Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	⌄ Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	i. + Add Selecione ; em seguida, introduza os parâmetros da política de instantâneos. ii. Selecione **Adicionar política**.

6. Se você quiser replicar seus snapshots para um cluster remoto, em **proteção remota**, selecione **replicar para um cluster remoto**.
   a. Selecione o cluster de origem e a VM de armazenamento e, em seguida, selecione a política de replicação.

      A transferência inicial de dados para replicação começa imediatamente por padrão.

7. Selecione **Guardar**.

Instantâneo da unidade de armazenamento

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja proteger.
3. Selecione ⋮ ; em seguida, selecione **proteger**. Se você quiser criar um instantâneo imediato sob demanda, em **proteção local**, selecione **Adicionar um instantâneo agora**.

A proteção local cria o instantâneo no mesmo cluster que contém a unidade de armazenamento.

4. Insira um nome para o instantâneo ou aceite o nome padrão; em seguida, opcionalmente, insira um rótulo SnapMirror.

   A etiqueta SnapMirror é utilizada pelo destino remoto.

5. Se você quiser criar snapshots automatizados usando uma política de snapshot, selecione **Agendar snapshots**.

   a. Selecione uma política de instantâneos.

      Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	i. + Add Selecione ; em seguida, introduza os parâmetros da política de instantâneos. ii. Selecione **Adicionar política**.

6. Se você quiser replicar seus snapshots para um cluster remoto, em **proteção remota**, selecione **replicar para um cluster remoto**.

   a. Selecione o cluster de origem e a VM de armazenamento e, em seguida, selecione a política de replicação.

      A transferência inicial de dados para replicação começa imediatamente por padrão.

7. Selecione **Guardar**.

O que se segue?

Agora que seus dados estão protegidos com snapshots, você deve "configurar a replicação de instantâneos"copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Gerenciar reserva de instantâneos

Saiba mais sobre a reserva de snapshots do ONTAP no armazenamento ASA r2.

A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Isso impede que os snapshots consumam espaço na sua unidade de armazenamento destinada aos dados do usuário.

A reserva de snapshots é definida como uma porcentagem do tamanho total da unidade de armazenamento.

Por exemplo, se a unidade de armazenamento for de 50 GB e você definir a reserva de snapshots para 10%, a quantidade de espaço reservada para snapshots será de 5 GB. Quando o espaço utilizado pelos snapshots atinge 5 GB, os snapshots mais antigos são excluídos automaticamente para liberar espaço para novos snapshots. Se o tamanho da unidade de armazenamento aumentar para 100 GB, a reserva de snapshots aumentará para 10 GB. A reserva máxima de snapshots que você pode definir é de 200%. Se sua unidade de armazenamento atingir o tamanho máximo de 128 TB, uma reserva de snapshots de 200% permite que você faça 2 snapshots completos.

Por padrão, a reserva de snapshots está definida como 0% e a exclusão automática de snapshots não está habilitada.

A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots padrão durante ou após a criação de unidades de armazenamento e durante a criação de grupos de consistência. Você também pode modificar a reserva de snapshots padrão em máquinas virtuais (VMs) de armazenamento existentes. No ONTAP 9.17.1 e versões anteriores, não é possível modificar essas configurações.

A reserva de snapshots é definida com a mesma porcentagem para todas as unidades de armazenamento em um grupo de consistência no momento em que o grupo de consistência é criado. A reserva de snapshots deve ser configurada individualmente em todas as unidades de armazenamento adicionadas posteriormente.

Modificar a reserva de snapshots em um sistema de armazenamento ASA r2

A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Por padrão, a reserva de snapshots está definida como 0%. A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots padrão da unidade de armazenamento e ativar a exclusão automática de snapshots. A exclusão automática de instantâneos está desativada por padrão. Quando um valor de reserva de snapshots é definido e a exclusão automática de snapshots está ativada, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Isso impede que os snapshots consumam espaço na sua unidade de armazenamento destinada aos dados do usuário.

"Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2.".

Modificar reserva de snapshots em unidades de armazenamento

Para definir valores de reserva de snapshots diferentes, configure cada unidade de armazenamento individualmente. Para usar o mesmo valor em todas as unidades de armazenamento, modifique a reserva de snapshots na máquina virtual de armazenamento.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o cursor sobre o nome da unidade de armazenamento para a qual deseja definir a reserva de snapshots.
3. Selecione ⋮ Em seguida, selecione **Editar**.
4. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots.
5. Verifique se a opção **Excluir automaticamente snapshots antigos** está selecionada.
6. Selecione **Guardar**.

Resultado

A reserva de snapshots está definida para a porcentagem que você especificou. Se o espaço consumido pelos snapshots atingir o limite reservado, os snapshots mais antigos serão excluídos automaticamente.

Modificar a reserva de snapshots em uma VM de armazenamento

Para definir a mesma reserva de snapshots para todas as unidades de armazenamento em uma VM de armazenamento, aplique a porcentagem desejada à VM de armazenamento. . Quando a reserva de snapshots é aplicada à máquina virtual de armazenamento, ela é aplicada a todas as unidades de armazenamento recém-criadas dentro da máquina virtual de armazenamento. Essa configuração não se aplica a unidades de armazenamento criadas antes da modificação da configuração.

Passos

1. No Gerenciador de Sistemas, selecione **Cluster > VMs de Armazenamento**; em seguida, selecione **Configurações**.
2. Em **Políticas**, ao lado de **Instantâneos**, selecione ⋮ Em seguida, selecione **Definir/editar reserva de instantâneo padrão**.
3. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots.
4. Verifique se a opção **Excluir automaticamente snapshots antigos** está selecionada.
5. Selecione **Guardar**.

Resultado

A reserva de snapshots para unidades de armazenamento recém-criadas é definida com a porcentagem especificada. Se a quantidade de espaço consumida pelos snapshots nessas unidades de armazenamento atingir a reserva, os snapshots mais antigos serão excluídos automaticamente.

Crie um relacionamento de pares de VMs de armazenamento intercluster em sistemas de armazenamento ASA r2

Um relacionamento de pares define conexões de rede que permitem que clusters e máquinas virtuais (VMs) de armazenamento troquem dados com segurança. Crie relacionamentos de pares entre VMs de armazenamento em diferentes clusters para permitir a proteção de dados e a recuperação de desastres usando o SnapMirror.

"Saiba mais sobre relacionamentos entre pares" .

Antes de começar

Você deve ter estabelecido um relacionamento de par de cluster entre os clusters local e remoto antes de poder criar um relacionamento de par de VM de armazenamento. "Criar um relacionamento de pares de cluster" se você ainda não o fez.

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. Em **Pares de VM de armazenamento** selecione **Adicionar um par de VM de armazenamento**.
3. Selecione a VM de armazenamento no cluster local; em seguida, selecione a VM de armazenamento no cluster remoto.
4. Selecione **Adicionar um peer de VM de armazenamento**.

Configurar a replicação de instantâneos

Replique snapshots para um cluster remoto a partir dos sistemas de storage ASA R2

A replicação de instantâneos é um processo no qual os grupos de consistência no seu sistema ASA R2 são copiados para um local remoto geograficamente. Após a replicação inicial, as alterações aos grupos de consistência são copiadas para o local remoto com base em uma política de replicação. Grupos de consistência replicados podem ser usados para recuperação de desastres ou migração de dados.

> ⓘ A replicação de instantâneos para um sistema de armazenamento ASA r2 só é suportada de e para outro sistema de armazenamento ASA r2. Não é possível replicar instantâneos de um sistema ASA r2 para um sistema ASA, AFF ou FAS ou de um sistema ASA, AFF ou FAS para um sistema ASA r2.

Para configurar a replicação Snapshot, é necessário estabelecer uma relação de replicação entre o sistema ASA R2 e o local remoto. A relação de replicação é regida por uma política de replicação. Uma política padrão para replicar todos os snapshots é criada durante a configuração do cluster. Você pode usar a política padrão ou, opcionalmente, criar uma nova política.

A partir do ONTAP 9.17.1, você pode aplicar políticas de replicação assíncrona a grupos de consistência em um relacionamento hierárquico. A replicação assíncrona não é suportada para grupos de consistência em relacionamentos hierárquicos no ONTAP 9.16.1.

"Saiba mais sobre grupos de consistência hierárquicos (pai/filho)" .

Passo 1: Crie um relacionamento de pares de cluster

Antes de proteger seus dados replicando-os em um cluster remoto, é necessário criar um relacionamento de peers de clusters entre o cluster local e o cluster remoto.

Antes de começar

Os pré-requisitos para peering de cluster são os mesmos para sistemas ASA r2 e outros sistemas ONTAP . "Revise os pré-requisitos para o peering de cluster" .

Passos

1. No cluster local, no System Manager, selecione **Cluster > Settings**.
2. Em **Intercluster Settings** ao lado de **Cluster Peers** selecione e, em seguida, selecione **Add a cluster peer**.
3. Selecione **Lauch Remote cluster**; isso gera uma senha que você usará para autenticar com o cluster remoto.
4. Depois que a frase-passe do cluster remoto for gerada, cole-a em **Passphrase** no cluster local.
5. Add Selecione ; em seguida, introduza o endereço IP da interface de rede entre clusters.
6. Selecione **Iniciar peering de cluster**.

O que se segue?

Você fez um pedido para o cluster ASA R2 local com um cluster remoto. Agora você pode criar uma relação de replicação.

Etapa 2: Opcionalmente, crie uma política de replicação personalizada

A política de replicação define quando as atualizações executadas no cluster ASA r2 são replicadas para o site remoto. O ONTAP inclui várias políticas de proteção de dados predefinidas que você pode usar para seus relacionamentos de replicação. Se as políticas predefinidas não atenderem às suas necessidades, você poderá criar uma política de replicação personalizada.

Aprenda sobre"políticas de proteção de dados ONTAP predefinidas" .

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas de replicação**.
2. + Add Selecione .
3. Introduza um nome para a política de replicação ou aceite o nome predefinido; em seguida, introduza uma descrição.
4. Selecione o **âmbito da política**.

   Se quiser aplicar a política de replicação a todo o cluster, selecione **Cluster**. Se desejar que a diretiva de replicação seja aplicada apenas às unidades de armazenamento em uma VM de armazenamento específica, selecione **Storage VM**.

5. Para o **Tipo de política**, selecione **Assíncrono**.

   Com a política assíncrona, os dados são copiados para o site remoto depois de serem gravados na origem. A replicação síncrona não é suportada para sistemas ASA r2.

6. Em **Transferir instantâneos da fonte**, aceite o agendamento de transferência padrão ou selecione outro.
7. Selecione para transferir todos os instantâneos ou para criar regras para determinar quais instantâneos transferir.
8. Opcionalmente, ative a compactação de rede.
9. Selecione **Guardar**.

O que se segue?

Você criou uma política de replicação e agora está pronto para criar uma relação de replicação entre o sistema ASA R2 e o local remoto.

Para mais informações

Saiba mais "VMs de armazenamento para acesso ao cliente"sobre o .

Passo 3: Crie uma relação de replicação

Uma relação de replicação de snapshot estabelece uma conexão entre o sistema ASA R2 e um local remoto para que você possa replicar grupos de consistência para um cluster remoto. Os grupos de consistência replicados podem ser usados para recuperação de desastres ou para migração de dados.

Para proteção contra ataques de ransomware, ao configurar sua relação de replicação, você pode optar por bloquear os snapshots de destino. Os instantâneos bloqueados não podem ser eliminados acidentalmente ou maliciosamente. Use snapshots bloqueados para recuperar dados se uma unidade de storage for comprometida por um ataque de ransomware.

Antes de começar

- "Saiba mais sobre políticas de replicação" .

Ao criar um relacionamento de replicação, você deve selecionar a política de replicação apropriada para seu relacionamento de replicação. Você pode usar uma política predefinida ou criar uma política personalizada.

- Se quiser bloquear os instantâneos de destino, tem de "Inicialize o relógio de conformidade do Snapshot" antes de criar a relação de replicação.

Crie uma relação de replicação com ou sem instantâneos de destino bloqueados.

Com instantâneos bloqueados

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione um grupo de consistência.
3. Selecione ; em seguida, selecione **proteger**.
4. Em **proteção remota**, selecione **replicar para um cluster remoto**.
5. Selecione a política **replicação**.

   Você deve selecionar uma política de replicação *Vault*.

6. Selecione **Definições de destino**.
7. Selecione **Bloquear instantâneos de destino para evitar a exclusão**
8. Introduza o período máximo e mínimo de retenção de dados.
9. Para atrasar o início da transferência de dados, desmarque **Iniciar transferência imediatamente**.

   A transferência inicial de dados começa imediatamente por padrão.

10. Opcionalmente, para substituir o agendamento de transferência padrão, selecione **Configurações de destino** e, em seguida, selecione **Substituir agendamento de transferência**.

    Seu plano de transferência deve ser de no mínimo 30 minutos para ser suportado.

11. Selecione **Guardar**.

Sem instantâneos bloqueados

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione para criar a relação de replicação com o destino local ou a origem local.

Opção	Passos
Destinos locais	a. Selecione **destinos locais** e, em seguida, Replicate selecione . b. Procure e selecione o grupo de consistência de origem. O grupo de consistência *source* refere-se ao grupo de consistência no cluster local que você deseja replicar.

Opção	Passos
Fontes locais	a. Selecione **fontes locais** e, em seguida, Replicate selecione . b. Procure e selecione o grupo de consistência de origem. c. Em **destino de replicação**, selecione o cluster para o qual replicar; em seguida, selecione a VM de armazenamento.

3. Selecione uma política de replicação.
4. Para atrasar o início da transferência de dados, selecione **Definições de destino**; em seguida, desmarque **Iniciar transferência imediatamente**.

   A transferência inicial de dados começa imediatamente por padrão.

5. Opcionalmente, para substituir o agendamento de transferência padrão, selecione **Configurações de destino** e, em seguida, selecione **Substituir agendamento de transferência**.

   Seu plano de transferência deve ser de no mínimo 30 minutos para ser suportado.

6. Selecione **Guardar**.

O que se segue?

Agora que você criou uma política de replicação e um relacionamento, sua transferência de dados inicial começa conforme definido na política de replicação. Opcionalmente, você pode testar o failover de replicação para verificar se o failover bem-sucedido pode ocorrer se o sistema ASA R2 ficar offline.

Etapa 4: Teste o failover de replicação

Opcionalmente, valide que você pode fornecer dados com êxito de unidades de armazenamento replicadas em um cluster remoto se o cluster de origem estiver offline.

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Passe o Mouse sobre a relação de replicação que você deseja testar e selecione .
3. Selecione **failover de teste**.
4. Insira as informações de failover e, em seguida, selecione **failover de teste**.

O que se segue?

Agora que seus dados estão protegidos com replicação snapshot para recuperação de desastres, você deve "criptografia de dados em repouso" fazê-lo para que não possa ser lido se um disco no sistema ASA R2 for reutilizado, devolvido, extraviado ou roubado.

Saiba mais sobre as políticas de proteção de dados predefinidas do ONTAP

A política de replicação define quando as atualizações executadas no cluster ASA r2 são replicadas para o site remoto. O ONTAP inclui várias políticas de proteção de dados predefinidas que você pode usar para seus relacionamentos de replicação.

Se as políticas predefinidas não atenderem às suas necessidades, você pode"criar uma política de replicação personalizada" .

Os sistemas ASA r2 não suportam replicação síncrona.

Os sistemas ASA r2 suportam as seguintes políticas de proteção predefinidas.

Política	Descrição	Tipo de política
Assíncrono	Uma política unificada de cofre e assíncrona do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais com um cronograma de transferência por hora.	Assíncrono
FailOverDuplex Automatizado	Política para SnapMirror síncrono com garantia de RTO zero e replicação de sincronização bidirecional.	Sincronização ativa do SnapMirror
CloudBackupPadrão	Política de cofre com regra diária.	Assíncrono
Backup diário	Política de cofre com uma regra diária e um cronograma de transferência diário.	Assíncrono
DPDefault	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo.	Assíncrono
MirrorAllSnapshots	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo.	Assíncrono
MirrorAllSnapshotsDiscardNetwork	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo, excluindo as configurações de rede.	Assíncrono
Espelho e Cofre	Uma política unificada assíncrona e de cofre do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais.	Assíncrono
Rede de descarte de espelho e cofre	Uma política unificada de cofre e assíncrona do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais, excluindo as configurações de rede.	Assíncrono
MirrorLatest	Política assíncrona do SnapMirror para espelhar o último sistema de arquivos ativo.	Assíncrono
Unified7year	Política unificada do SnapMirror com retenção de 7 anos.	Assíncrono
XDPPadrão	Política de cofre com regras diárias e semanais.	Assíncrono

Interrompa um relacionamento de replicação assíncrona no seu sistema ASA r2

Em certas situações, pode ser necessário interromper um relacionamento de replicação assíncrona. Por exemplo, se você estiver executando o ONTAP 9.16.1 e quiser aumentar o tamanho de um grupo de consistência que está em um relacionamento de replicação

assíncrona, será necessário quebrar o relacionamento antes de poder modificar o tamanho do grupo de consistência.

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **Destinos locais** ou **Fontes locais**.
3. Ao lado do relacionamento que você deseja interromper, selecione ⋮ ; então selecione **Quebrar**.
4. Selecione **Quebrar**.

Resultado

O relacionamento assíncrono entre o grupo de consistência primário e secundário é quebrado.

Configurar sincronização ativa do SnapMirror

Fluxo de trabalho de configuração de sincronização ativa do SnapMirror

A proteção de dados de sincronização ativa do ONTAP SnapMirror permite que os serviços empresariais continuem operando mesmo em caso de falha total do site, permitindo que os aplicativos realizem failover de forma transparente usando uma cópia secundária. Com a sincronização ativa do SnapMirror , não é necessária intervenção manual ou script personalizado para acionar um failover.

Embora os procedimentos do System Manager para configurar a sincronização ativa do SnapMirror sejam diferentes em sistemas ASA r2 do que em sistemas NetApp FAS, AFF e ASA que executam a personalidade ONTAP unificada, os requisitos, a arquitetura e a operação da sincronização ativa do SnapMirror são os mesmos.

"Saiba mais sobre as personalidades da ONTAP" .

> ⓘ A partir do ONTAP 9.18.1, a sincronização ativa do SnapMirror é suportada em configurações de quatro nós. No ONTAP 9.17.1, a sincronização ativa do SnapMirror é suportada apenas em configurações de dois nós.

"Saiba mais sobre a sincronização ativa do SnapMirror" .

"Saiba mais sobre recuperação de desastres com sincronização ativa SnapMirror no seu sistema ASA r2"

Em sistemas ASA r2, a sincronização ativa do SnapMirror suporta configurações simétricas ativa/ativa. Em uma configuração simétrica ativa/ativa, ambos os sites podem acessar o armazenamento local para E/S ativa.

Saiba mais sobre "configurações simétricas ativas/ativas" .

1 Prepare-se para configurar a sincronização ativa do SnapMirror .

Para "prepare-se para configurar a sincronização ativa do SnapMirror" no seu sistema ASA r2, você deve revisar os pré-requisitos de configuração, confirmar o suporte para seus sistemas operacionais host e estar ciente dos limites de objetos que podem afetar a configuração específica.

2 **Confirme a configuração do seu cluster.**

Antes de configurar a sincronização ativa do SnapMirror , você deve "confirme se seus clusters ASA r2 estão nos relacionamentos de peering adequados e atendem a outros requisitos de configuração" .

3 **Instale o ONTAP Mediator.**

Você pode usar o ONTAP Mediator ou o ONTAP Cloud Mediator para monitorar a integridade do seu cluster e garantir a continuidade dos negócios. Se estiver usando o ONTAP Mediator, você deve: "instale-o" no seu host. Se estiver usando o ONTAP Cloud Mediator, você pode pular esta etapa.

4 **Configure o ONTAP Mediator ou o ONTAP Cloud Mediator usando certificados autoassinados.**

Você deve "configurar o mediador ONTAP ou o mediador de nuvem ONTAP" antes de poder começar a usá-lo com o SnapMirror Active Sync para monitoramento de cluster.

5 **Configurar sincronização ativa do SnapMirror .**

"Configurar sincronização ativa do SnapMirror" para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente no caso de um desastre.

Preparar para configurar a sincronização ativa do SnapMirror em sistemas ASA r2

Para se preparar para configurar a sincronização ativa do SnapMirror no seu sistema ASA r2, você deve revisar os pré-requisitos de configuração, confirmar o suporte para os sistemas operacionais dos seus hosts e estar ciente dos limites de objetos que podem afetar a configuração específica.

Passos

1. Revise a sincronização ativa do SnapMirror "pré-requisitos" .
2. "Confirme se os sistemas operacionais do seu host são suportados" para sincronização ativa do SnapMirror .
3. Revise o "limites do objeto" que podem impactar sua configuração.
4. Verifique o suporte do protocolo do host para sincronização ativa do SnapMirror no seu sistema ASA r2.

   O suporte para sincronização ativa do SnapMirror em sistemas ASA r2 varia de acordo com a versão do ONTAP e o protocolo do host.

Começando com ONTAP…	A sincronização ativa do SnapMirror suporta…
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP

Começando com ONTAP…	A sincronização ativa do SnapMirror suporta…
9.16.0	• iSCSI • FC

Limitações do protocolo NVMe com sincronização ativa SnapMirror em sistemas ASA r2

Antes de configurar a sincronização ativa do SnapMirror em um sistema ASA r2 com hosts NVMe, você deve estar ciente de certas limitações do protocolo NVMe.

Todas as unidades de armazenamento NVMe no subsistema NVMe devem ser membros do mesmo grupo de consistência e devem fazer parte do mesmo relacionamento de sincronização ativa do SnapMirror .

Os protocolos NVMe/FC e NVMe/TCP são suportados com sincronização ativa do SnapMirror da seguinte forma:

- Somente em clusters de 2 nós
- Somente em hosts ESXi
- Somente com configurações simétricas ativas/ativas

  Configurações ativas/ativas assimétricas não são suportadas com hosts NVMe.

A sincronização ativa do SnapMirror com NVMe não oferece suporte ao seguinte:

- Subsistemas mapeados para mais de um grupo de consistência

  Um grupo de consistência pode ser mapeado com vários subsistemas, mas cada subsistema pode ser mapeado para apenas um grupo de consistência.

- Expansão de grupos de consistência em um relacionamento de sincronização ativa do SnapMirror
- Mapeando unidades de armazenamento NVMe que não estão em um relacionamento de sincronização ativa do SnapMirror para subsistemas replicados
- Removendo uma unidade de armazenamento de um grupo de consistência
- Mudança de geometria do grupo de consistência
- "Transferência de dados descarregados da Microsoft (ODX)"

O que vem a seguir?

Depois de concluir a preparação necessária para habilitar a sincronização ativa do SnapMirror , você deve "confirme a configuração do seu cluster" .

Confirme a configuração do cluster ASA r2 antes de configurar a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror depende de clusters pareados para proteger seus dados em caso de failover. Antes de configurar a sincronização ativa do SnapMirror , você deve confirmar se seus clusters ASA r2 estão em um relacionamento de pareamento compatível e atendem a outros requisitos de configuração.

Passos

1. Confirme se existe um relacionamento de peering de cluster entre os clusters.

   > O espaço IP padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos entre pares de cluster. Um espaço IP personalizado não é suportado.

   "Criar um relacionamento de pares de cluster" .

2. Confirme se existe um relacionamento de mesmo nível entre as máquinas virtuais de armazenamento (VMs) em cada cluster.

   "Criar um relacionamento entre pares de VMs de armazenamento entre clusters" .

3. Confirme se pelo menos um LIF foi criado em cada nó do cluster.

   "Criar um LIF".

4. Confirme se as unidades de armazenamento necessárias foram criadas e mapeadas para grupos de hosts.

   "Criar uma unidade de armazenamento" e "mapear a unidade de armazenamento para um grupo de hosts" .

5. Examine novamente o host do aplicativo para descobrir novas unidades de armazenamento.

O que se segue?

Depois de confirmar a configuração do cluster, você estará pronto para "instalar o ONTAP Mediator" .

Instalar o ONTAP Mediator em sistemas ASA r2

Para instalar o ONTAP Mediator no seu sistema ASA r2, você deve seguir o mesmo procedimento usado para instalar o ONTAP Mediator em todos os outros sistemas ONTAP .

A instalação do ONTAP Mediator inclui a preparação para a instalação, a ativação do acesso aos repositórios, o download do pacote do ONTAP Mediator, a verificação da assinatura do código, a instalação do pacote no host e a execução de tarefas pós-instalação.

Para instalar o ONTAP Mediator, siga "este fluxo de trabalho"

O que vem a seguir

Após a instalação do ONTAP Mediator, você deve "configurar o ONTAP Mediator usando certificados autoassinados" .

Configurar o ONTAP Mediator ou o ONTAP Cloud Mediator em sistemas ASA r2

Você deve configurar o ONTAP Mediator ou o ONTAP Cloud Mediator antes de começar a usar a sincronização ativa do SnapMirror para monitoramento de cluster. O ONTAP Mediator e o ONTAP Cloud Mediator fornecem um armazenamento persistente e protegido para metadados de alta disponibilidade (HA) usados pelos clusters ONTAP em um relacionamento de sincronização ativa do SnapMirror . Além disso, ambos os mediadores fornecem uma funcionalidade de consulta de integridade de nó síncrona para auxiliar na determinação de quorum e servem como um proxy de ping para

detecção de atividade do controlador.

Antes de começar

Se você estiver usando o ONTAP Cloud Mediator, verifique se o seu sistema ASA r2 atende aos requisitos "pré-requisitos" .

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione **Adicionar um mediador**.
3. Selecione o **Tipo de mediador**.
4. Para um mediador **na nuvem**, insira o ID da organização, o ID do cliente e o segredo do cliente. Para um mediador **local**, insira o endereço IP, a porta, o nome de usuário e a senha do mediador.
5. Selecione o peer de cluster na lista de peers de cluster qualificados ou selecione **Adicionar um peer de cluster** para adicionar um novo.
6. Adicione as informações do certificado
   - Se você estiver usando um certificado autoassinado, copie o conteúdo do `intermediate.crt` arquivo e cole-o no campo **Certificado** ou selecione **Importar** para navegar até o `intermediate.crt` arquivar e importar as informações do certificado.
   - Se você estiver usando um certificado de terceiros, insira as informações do certificado no campo **Certificado**.
7. Selecione **Adicionar**.

O que se segue?

Depois de inicializar o mediador, você pode "configurar sincronização ativa do SnapMirror" para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente em caso de desastre.

Configurar a sincronização ativa do SnapMirror em sistemas ASA r2

Configure a sincronização ativa do SnapMirror para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente em caso de desastre.

Em sistemas ASA r2, a sincronização ativa do SnapMirror suporta configurações simétricas ativa/ativa. Em uma configuração simétrica ativa/ativa, ambos os sites podem acessar o armazenamento local para E/S ativa.

> Se você estiver usando o protocolo iSCSI ou FC e usar ferramentas ONTAP para VMware Sphere, você pode opcionalmente "use o ONTAP Tools para VMware para configurar a sincronização ativa do SnapMirror" .

Antes de começar

"Criar um grupo de consistência" no site primário com novas unidades de armazenamento. Se você quiser criar uma configuração ativa/ativa simétrica não uniforme, crie também um grupo de consistência no site secundário com novas unidades de armazenamento.

Saiba mais sobre "não uniforme" configurações simétricas ativas/ativas.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o mouse sobre o nome do grupo de consistência que você deseja proteger com a sincronização ativa do SnapMirror .
3. Selecione ⋮ e então selecione **Proteger**.
4. Em **proteção remota**, selecione **replicar para um cluster remoto**.
5. Selecione um peer de cluster existente ou escolha **Adicionar um novo**.
6. Selecione a VM de armazenamento.
7. Para a política de replicação, selecione **AutomatedFailOverDuplex**.
8. Se você estiver criando uma configuração ativa/ativa simétrica não uniforme, selecione **Configurações de destino**; em seguida, insira o nome do novo grupo de consistência de destino criado antes de iniciar este procedimento.
9. Selecione **Guardar**.

Resultado

A sincronização ativa do SnapMirror é configurada para proteger seus dados para que você possa continuar as operações com objetivo de ponto de recuperação próximo de zero (RPO) e objetivo de tempo de recuperação próximo de zero (RTO) em caso de desastre.

Gerenciar sincronização ativa do SnapMirror

Reconfigure o ONTAP Mediator ou o ONTAP Cloud Mediator para usar um certificado de terceiros em sistemas ASA r2

Se você configurar o ONTAP Mediator ou o ONTAP Cloud Mediator com um certificado autoassinado, poderá reconfigurar o mediador para usar um certificado de terceiros. Certificados de terceiros podem ser preferidos ou exigidos pela sua organização por motivos de segurança.

Etapa 1: remover a configuração do mediador

Para reconfigurar o mediador, você deve primeiro remover sua configuração atual do cluster.

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione ⋮ ao lado do peer de cluster com a configuração do mediador que você deseja remover; em seguida, selecione **Remover**.

   Se você tiver vários mediadores instalados e quiser remover todas as configurações, selecione ⋮ ao lado de **Mediadores**; depois selecione **Remover**.
3. Selecione **Remover** para confirmar que deseja remover a configuração do mediador.

Etapa 2: remover o certificado autoassinado

Após a remoção da configuração do mediador, você deve remover o certificado autoassinado associado do cluster.

Passos

1. Selecione **Cluster > Settings**.

2. Em **Segurança**, selecione **Certificados**.
3. Selecione o certificado que você deseja remover.
4. Selecione ⋮ ; em seguida, selecione **Delete**.

Etapa 3: Reinstale o mediador com um certificado de terceiros

Depois de remover o certificado autoassinado associado, você pode reconfigurar o mediador com o certificado de terceiros.

Passos

1. Selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione **Adicionar um mediador**.
3. Selecione o **Tipo de mediador**.
4. Para um mediador **na nuvem**, insira o ID da organização, o ID do cliente e o segredo do cliente. Para um mediador **local**, insira o endereço IP, a porta, o nome de usuário do mediador e a senha do mediador.
5. Selecione um peer de cluster na lista de peers de cluster qualificados ou selecione **Adicionar um peer de cluster** para adicionar um novo.
6. Em **Certificado**, insira as informações do certificado de terceiros.
7. Selecione **Adicionar**.

Resultado

O ONTAP Mediator ou o ONTAP Cloud Mediator é reconfigurado para usar o certificado de terceiros. Agora você pode usar o mediador para gerenciar relacionamentos de sincronização ativos do SnapMirror .

Executar um failover planejado de clusters ASA r2 em um relacionamento de sincronização ativa do SnapMirror

O SnapMirror Active Sync oferece disponibilidade contínua para aplicativos críticos de negócios, criando uma cópia dos seus dados em um site secundário e permitindo que seus aplicativos host façam failover de forma automática e transparente em caso de desastre. Pode ser necessário executar um failover planejado do seu relacionamento com o SnapMirror Active Sync para testar o processo de failover ou realizar manutenção no site principal.

Antes de começar

- O relacionamento de sincronização ativa do SnapMirror deve estar sincronizado.
- Não é possível iniciar um failover planejado quando uma operação não disruptiva, como uma movimentação de unidade de armazenamento, estiver em andamento.
- O ONTAP Mediator ou ONTAP Cloud Mediator deve estar configurado, conectado e em quorum.

Passos

1. Selecione **Proteção > Replicação**.
2. Selecione o relacionamento de sincronização ativa do SnapMirror no qual você deseja fazer failover.
3. Selecione ⋮ ; então selecione **Failover**.

O que vem a seguir

Use o `snapmirror failover show` comando na interface de linha de comando (CLI) do ONTAP para monitorar o status do failover.

Reestabeleça o relacionamento de sincronização ativa do SnapMirror após um failover não planejado de seus clusters ASA r2

Nos sistemas ASA r2, SnapMirror active sync suporta configurações ativo-ativo simétricas. Em uma configuração ativo-ativo simétrica, ambos os sites podem acessar o armazenamento local para E/S ativa. Se o cluster de origem falhar ou for isolado, o mediador aciona um failover automático não planejado (AUFO) e processa todas as operações de E/S do cluster de destino até que o cluster de origem se recupere.

Se você experimentar um AUFO da sua relação de sincronização ativa SnapMirror, você deve restabelecer a relação e retomar as operações no cluster de origem assim que ele voltar a ficar online.

Antes de começar

- O relacionamento de sincronização ativa do SnapMirror deve estar sincronizado.
- Não é possível iniciar um failover planejado quando uma operação não disruptiva, como uma movimentação de unidade de armazenamento, estiver em andamento.
- O Mediador ONTAP deve estar configurado, conectado e em quorum.
- Para recuperar caminhos de E/S perdidos ou atualizar os estados dos caminhos de E/S em seus hosts, você precisa executar uma nova verificação de armazenamento/adaptador nos hosts após o cluster de armazenamento primário retomar a operação.

Passos

1. Selecione **Proteção > Replicação**.
2. Selecione o relacionamento de sincronização ativa do SnapMirror que você precisa restabelecer.
3. Aguarde até que o status do relacionamento exiba **InSync**.
4. Selecione ⋮ ; em seguida, selecione **Failover** para retomar as operações no cluster primário original.

Excluir um relacionamento de sincronização ativo do SnapMirror no seu sistema ASA r2

Se você não precisar mais de RPO e RTO próximos de zero para um aplicativo comercial, remova a proteção de sincronização ativa do SnapMirror excluindo o relacionamento de sincronização ativa do SnapMirror associado. Se você estiver executando o ONTAP 9.16.1 em um sistema ASA r2, talvez também seja necessário excluir o relacionamento de sincronização ativa do SnapMirror antes de poder fazer determinadas alterações de geometria em grupos de consistência em um relacionamento de sincronização ativa do SnapMirror .

Etapa 1: encerrar a replicação do host

Se o grupo de hosts do cluster de origem for replicado para o cluster de destino e os grupos de consistência de destino forem mapeados para o grupo de hosts replicado, você deverá encerrar a replicação de hosts no cluster de origem antes de poder excluir o relacionamento de sincronização ativa do SnapMirror .

Passos

1. No System Manager, selecione **Host**.

2. Ao lado de um host que contém o grupo de hosts que você deseja parar de replicar, selecione e, em seguida, selecione **Editar**.
3. Desmarque **Replicar configuração do host** e selecione **Atualizar**.

Etapa 2: Excluir o relacionamento de sincronização ativa do SnapMirror

Para remover a proteção de sincronização ativa do SnapMirror de um grupo de consistência, você deve excluir o relacionamento de sincronização ativa do SnapMirror .

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **Destinos locais** ou **Fontes locais**.
3. Ao lado do relacionamento de sincronização ativa do SnapMirror que você deseja remover, selecione ; então selecione **Excluir**.
4. Selecione **Liberar os instantâneos base do grupo de consistência de origem**.
5. Selecione **Eliminar**.

Resultado

O relacionamento de sincronização ativa do SnapMirror é removido e os instantâneos base do grupo de consistência de origem são liberados. As unidades de armazenamento no grupo de consistência não são mais protegidas pela sincronização ativa do SnapMirror .

O que se segue?

"Configurar a replicação de instantâneos"para copiar o grupo de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Remova o ONTAP Mediator ou o ONTAP Cloud Mediator do seu sistema ASA r2

Você pode usar apenas um tipo de mediador por vez para sincronização ativa do SnapMirror no seu sistema ASA r2. Se você optar por alterar seu tipo de mediador, deverá remover sua instância atual antes de instalar outra instância.

Passos

Você deve usar a interface de linha de comando (CLI) do ONTAP para remover o ONTAP Mediator ou o ONTAP Cloud Mediator.

Mediador ONTAP

1. Remover o Mediador ONTAP :

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   Exemplo:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

Mediador de Nuvem ONTAP

1. Remover o ONTAP Cloud Mediator:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   Exemplo:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Informações relacionadas

- "remover mediador snapmirror"

Restaure os dados em sistemas de storage ASA R2

Os dados em um grupo de consistência ou unidade de armazenamento protegida por instantâneos podem ser restaurados se forem perdidos ou corrompidos.

Restaure um grupo de consistência

A restauração de um grupo de consistência substitui os dados em todas as unidades de storage do grupo de consistência pelos dados de um snapshot. As alterações feitas nas unidades de armazenamento após a criação do instantâneo não são restauradas.

É possível restaurar um grupo de consistência a partir de um instantâneo local ou remoto.

Restaurar a partir de um instantâneo local

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Clique duas vezes no grupo de consistência que contém os dados que você precisa restaurar.

   Abre-se a página de detalhes do grupo de consistência.

3. Selecione **Snapshots**.
4. Selecione o instantâneo que pretende restaurar e, em seguida, selecione .
5. Selecione **Restore consistency group from this snapshot**; then Select **Restore**.

Restaurar a partir de um instantâneo remoto

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **destinos locais**.
3. Selecione **fonte** que deseja restaurar e selecione .
4. Selecione **Restaurar**.
5. Selecione o cluster, a VM de armazenamento e o grupo de consistência para o qual você deseja restaurar os dados.
6. Selecione o instantâneo a partir do qual pretende restaurar.
7. Quando solicitado, digite "Restore" (restaurar); em seguida, selecione **Restore** (Restaurar).

Resultado

Seu grupo de consistência é restaurado ao ponto no tempo do snapshot usado para restauração.

Restaurar uma unidade de armazenamento

A restauração de uma unidade de armazenamento substitui todos os dados da unidade de armazenamento pelos dados de um instantâneo. As alterações efetuadas na unidade de armazenamento após a criação do instantâneo não são restauradas.

Passos

1. No System Manager, selecione **Storage**.
2. Faça duplo clique na unidade de armazenamento que contém os dados que necessita de restaurar.

   Abre-se a página de detalhes da unidade de armazenamento.

3. Selecione **Snapshots**.
4. Selecione o instantâneo que pretende restaurar.
5. Selecione ; em seguida, selecione **Restore**.
6. Selecione **Use este instantâneo para restaurar a unidade de armazenamento**; em seguida, selecione **Restore**.

Resultado

Sua unidade de armazenamento é restaurada até o ponto no tempo do instantâneo usado para restauração.

Gerenciar grupos de consistência

Saiba mais sobre grupos de consistência ONTAP em sistemas de armazenamento ASA r2

Um grupo de consistência é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade. Use grupos de consistência para simplificar o gerenciamento de armazenamento.

Por exemplo, suponha que você tenha um banco de dados com 10 unidades de armazenamento em um grupo de consistência e precise fazer backup de todo o banco de dados. Em vez de fazer backup de cada unidade de armazenamento, você pode fazer backup de todo o banco de dados simplesmente adicionando proteção de dados de instantâneo ao grupo de consistência. Fazer backup das unidades de armazenamento como um grupo de consistência em vez de individualmente também fornece um backup consistente de todas as unidades, enquanto fazer backup das unidades individualmente pode criar inconsistências.

A partir do ONTAP 9.16.1, você pode usar o System Manager para criar grupos de consistência hierárquicos no seu sistema ASA r2. Em uma estrutura hierárquica, um ou mais grupos de consistência são configurados como filhos em um grupo de consistência pai.

Os grupos hierárquicos de consistência permitem que você aplique políticas de snapshot individuais a cada grupo filho de consistência e replique os snapshots de todos os grupos filhos de consistência a um cluster remoto como uma única unidade replicando o pai. Isso simplifica a proteção e o gerenciamento de dados para estruturas de dados complexas. Por exemplo, suponha que você crie um grupo de consistência pai chamado `SVM1_app` que contém dois grupos de consistência filhos: `SVM1app_data` Para dados de aplicativos e `SVM1app_logs` para logs de aplicativos. Os instantâneos de `SVM1app_data` são tirados a cada 15 minutos e os instantâneos de são tirados a `SVM1app_logs` cada hora. O grupo de consistência pai `SVM1_app,` tem uma política do SnapMirror que replica os snapshots de ambos `SVM1app_data` e `SVM1app_logs` para um cluster remoto a cada 24 horas. O grupo de consistência pai `SVM1_app` é gerenciado como uma única unidade e os grupos de consistência filho são gerenciados como unidades separadas.

Grupos de consistência em relacionamentos de replicação

A partir do ONTAP 9.17.1, você pode fazer as seguintes alterações de geometria em grupos de consistência em um relacionamento de replicação assíncrona ou em um relacionamento de sincronização ativa do SnapMirror sem interromper ou excluir o relacionamento. Quando ocorre uma alteração de geometria no grupo de consistência primário, a alteração é replicada para o grupo de consistência secundário.

- "Modificar o tamanho de uma unidade de armazenamento"adicionando ou removendo unidades de armazenamento.
- "Promova um único grupo de consistência"para um grupo de consistência pai.
- "Rebaixar um grupo de consistência pai"para um único grupo de consistência.
- "Desanexar um grupo de consistência filho"de um grupo de consistência pai.
- "Crie um grupo de consistência filho"usando um grupo de consistência existente.

No ONTAP 9.16.1, você deve"quebrar o relacionamento de replicação assíncrona" e"excluir o relacionamento de sincronização ativa do SnapMirror" antes de fazer alterações de geometria no grupo de consistência.

Proteja grupos de consistência no seu sistema ASA r2 com instantâneos

Crie instantâneos dos grupos de consistência no seu sistema de armazenamento ASA r2 para proteger os dados nas unidades de armazenamento que fazem parte do grupo de

consistência. Se não precisar mais proteger os dados em nenhuma das unidades de armazenamento no grupo de consistência, você poderá remover a proteção de instantâneo do grupo de consistência.

Se não precisar mais proteger os dados de unidades de armazenamento específicas no grupo de consistência, você poderá remover essas unidades de armazenamento do grupo de consistência.

Adicionar proteção de dados de snapshot a um grupo de consistência

Quando você adiciona proteção de dados de snapshot a um grupo de consistência, os snapshots locais do grupo de consistência são feitos em intervalos regulares com base em uma programação predefinida.

Você pode usar snapshots que "restaurar dados"estão perdidos ou corrompidos.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja proteger.
3. Selecione ; em seguida, selecione **Editar**.
4. Em **proteção local**, selecione **Agendar instantâneos**.
5. Selecione uma política de instantâneos.

   Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	a. Add Selecione ; em seguida, introduza o novo nome da política. b. Selecione o escopo da política. c. Em **horários**, Add selecione . d. Selecione o nome que aparece em **Nome da agenda**; em seguida, selecione . e. Selecione o agendamento da política. f. Em **máximo de instantâneos**, insira o número máximo de instantâneos que você deseja manter do grupo de consistência. g. Opcionalmente, sob **SnapMirror label**, digite um rótulo SnapMirror. h. Selecione **Guardar**.

6. Selecione **Guardar**.

O que vem a seguir

Agora que seus dados estão protegidos com snapshots, você deve "configurar a replicação de instantâneos"copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Remova a proteção de dados do snapshot de um grupo de consistência

Quando você remove a proteção de dados de snapshot de um grupo de consistência, os snapshots são desabilitados para todas as unidades de armazenamento no grupo de consistência.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja parar de proteger.
3. Selecione ⋮ ; em seguida, selecione **Editar**.
4. Em **proteção local**, desmarque Agendar instantâneos.
5. Selecione **Editar**.

Resultado

Os instantâneos não serão tirados para nenhuma das unidades de armazenamento no grupo consistência.

Modifique o tamanho dos grupos de consistência no seu sistema ASA r2

Aumente ou diminua o tamanho de um grupo de consistência modificando o número de unidades de armazenamento no grupo de consistência.

Adicione unidades de armazenamento a um grupo de consistência

Expanda a quantidade de armazenamento gerenciado por um grupo de consistência adicionando unidades de armazenamento novas ou existentes ao grupo.

A partir do ONTAP 9.18.1, você pode configurar a reserva de snapshots e a exclusão automática de snapshots para limitar a quantidade de espaço usada pelos snapshots em suas unidades de armazenamento. Ao adicionar uma unidade de armazenamento a um grupo de consistência existente, a reserva de snapshots e a exclusão automática de snapshots são definidas da seguinte forma por padrão.

Se você adicionar…	A porcentagem de reserva instantânea está definida como…	A exclusão automática de instantâneos é…
Novas unidades de armazenamento	0	Desabilitado
Unidades de armazenamento existentes	Inalterado	Inalterado

Você pode modificar as configurações padrão para novas unidades de armazenamento ao criá-las. Você também pode"modificar unidades de armazenamento existentes" para atualizar suas configurações atuais.

"Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2.".

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja expandir estiver em um relacionamento de sincronização ativo do SnapMirror , você deve"excluir o relacionamento de sincronização ativa do SnapMirror" antes de poder adicionar unidades de armazenamento. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve"romper o relacionamento" antes de poder expandir o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Adicionar unidades de armazenamento existentes

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja expandir.
3. Selecione ⋮ ; em seguida, selecione **expandir**.
4. Selecione **usando unidades de armazenamento existentes**.
5. Selecione as unidades de armazenamento a serem adicionadas ao grupo de consistência; em seguida, selecione **expandir**.

Adicione novas unidades de armazenamento

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja expandir.
3. Selecione ⋮ ; em seguida, selecione **expandir**.
4. Selecione **usando novas unidades de armazenamento**.
5. Introduza o número de unidades que pretende criar e a capacidade por unidade.

   Se você criar mais de uma unidade, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host. Para atribuir uma capacidade diferente a cada unidade, selecione **Adicionar uma capacidade diferente**.

6. Selecione **expandir**.

O que vem a seguir

Depois de criar uma nova unidade de armazenamento, "adicione iniciadores de host"deverá e "mapeie a unidade de armazenamento recém-criada para um host". A adição de iniciadores de host torna os hosts elegíveis para acessar as unidades de armazenamento e executar operações de dados. O mapeamento de uma unidade de armazenamento para um host permite que a unidade de armazenamento comece a fornecer dados para o host para o qual está mapeado.

O que se segue?

Os instantâneos existentes do grupo de consistência não incluem as unidades de armazenamento recém-adicionadas. Você deve "crie um instantâneo imediato"do seu grupo de consistência para proteger suas unidades de storage recém-adicionadas até que o próximo snapshot agendado seja criado automaticamente.

Remova uma unidade de armazenamento de um grupo de consistência

Remova uma unidade de armazenamento de um grupo de consistência para excluí-la, gerenciá-la como parte de um grupo de consistência diferente ou interromper a proteção de seus dados. Remover uma unidade de armazenamento de um grupo de consistência rompe a relação entre a unidade de armazenamento e o grupo de consistência, mas não exclui a unidade de armazenamento.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Clique duas vezes no grupo de consistência do qual você deseja remover uma unidade de armazenamento.

3. Na seção **Visão geral**, em **unidades de armazenamento**, selecione a unidade de armazenamento que deseja remover; em seguida, selecione **Remover do grupo de consistência**.

Resultado

A unidade de armazenamento já não é membro do grupo de consistência.

O que vem a seguir

Se precisar continuar a proteção de dados para a unidade de armazenamento, adicione a unidade de armazenamento a outro grupo de consistência.

Excluir grupos de consistência no seu sistema ASA r2

Se não precisar mais gerenciar os membros de um grupo de consistência como uma única unidade, você poderá excluir o grupo de consistência. Depois que um grupo de consistência é excluído, as unidades de armazenamento que estavam anteriormente no grupo permanecem ativas no cluster. Se o grupo de consistência estiver em um relacionamento de replicação, as cópias replicadas permanecerão no cluster remoto.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja excluir estiver em um relacionamento de sincronização ativo do SnapMirror , você deverá"excluir o relacionamento de sincronização ativa do SnapMirror" antes de excluir o grupo de consistência. Excluir esse relacionamento antes de modificar um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja excluir.
3. Selecione ⋮ ; em seguida, selecione **Delete**.
4. Aceite o aviso e, em seguida, selecione **Delete**.

O que se segue?

Depois de excluir um grupo de consistência, as unidades de armazenamento anteriormente no grupo de consistência não serão mais protegidas por instantâneos. Considere adicionar essas unidades de armazenamento a outro grupo de consistência para protegê-las contra a perda de dados.

Gerenciar grupos de consistência hierárquica no seu sistema ASA r2

A partir do ONTAP 9.16.1, você pode usar o System Manager para criar grupos de consistência hierárquicos no seu sistema ASA r2. Em uma estrutura hierárquica, um ou mais grupos de consistência são configurados como filhos em um grupo de consistência pai. Você pode aplicar políticas de instantâneos individuais a cada grupo de consistência filho e replicar os instantâneos de todos os grupos de consistência filho para um cluster remoto como uma única unidade replicando o pai. Isso simplifica a proteção e o gerenciamento de dados para estruturas de dados complexas.

Promover um grupo de consistência existente para um grupo de consistência pai

Se você promover um grupo de consistência existente para um pai, um novo grupo de consistência filho será criado e as unidades de armazenamento pertencentes ao grupo de consistência promovido serão movidas

para o novo grupo de consistência filho. Unidades de armazenamento não podem ser associadas diretamente a um grupo de consistência pai.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja promover estiver em um relacionamento de sincronização ativa do SnapMirror , você deve"excluir o relacionamento de sincronização ativa do SnapMirror" antes que o grupo de consistência possa ser promovido. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve"romper o relacionamento" antes de poder promover o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de promover um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja converter em um grupo de consistência pai.
3. Selecione ; em seguida, selecione **promover para o grupo de consistência pai**.
4. Insira um nome para o novo grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione **promover**.

O que se segue?

Você pode criar grupos de consistência filhos adicionais sob o grupo de consistência pai. Você também pode"configurar a replicação de instantâneos" para copiar os grupos de consistência pai e filho para um local geograficamente remoto para backup e recuperação de desastres.

Demote um grupo de consistência pai para um único grupo de consistência

Quando você rebaixa um grupo de consistência pai para um único grupo de consistência, as unidades de armazenamento dos grupos de consistência filho associados são adicionadas ao grupo de consistência pai. Os grupos de consistência filhos são excluídos e o pai é então gerenciado como um único grupo de consistência.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja rebaixar estiver em um relacionamento de sincronização ativa do SnapMirror , você deve"excluir o relacionamento de sincronização ativa do SnapMirror" antes que o grupo de consistência possa ser rebaixado. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve"romper o relacionamento" antes de poder rebaixar o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência pai que você deseja rebaixar.
3. Selecione ; em seguida, selecione **demote para um único grupo de consistência**.
4. Selecione **demote**

O que se segue?

"Adicionar uma política de instantâneos" para o grupo de consistência rebaixado para proteger as unidades de

armazenamento que foram gerenciadas anteriormente pelos grupos de consistência infantil.

Crie um grupo de consistência filho

A criação de grupos de consistência filho permite que você aplique políticas de instantâneo individuais a cada filho. A partir do ONTAP 9.17.1, você também pode aplicar políticas de replicação individuais diretamente a cada filho. No ONTAP 9.16.1, as políticas de replicação podem ser aplicadas somente no nível pai.

Você pode criar um grupo de consistência filho a partir de um grupo de consistência novo ou existente.

De um novo grupo de consistência

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência pai ao qual você deseja adicionar um grupo de consistência filho.
3. Selecione ⋮ ; em seguida, selecione **Adicionar um novo grupo de consistência filho**.
4. Insira um nome para o grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione para adicionar unidades de armazenamento existentes ao grupo de consistência filho ou para criar novas unidades de armazenamento.

   Se criar novas unidades de armazenamento, introduza o número de unidades que pretende criar e a capacidade por unidade; em seguida, introduza as informações do anfitrião.

   Se você criar mais de uma unidade de armazenamento, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host. Para atribuir uma capacidade diferente a cada unidade, selecione **Adicionar uma capacidade diferente**.

6. Selecione **Adicionar**.

De um grupo de consistência existente

Antes de começar

Se o grupo de consistência que você deseja usar já for filho de outro grupo de consistência, você deve"desconectá-lo do grupo de consistência pai existente" antes de poder movê-lo para um novo grupo de consistência pai.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione o grupo de consistência existente que você gostaria de criar um grupo de consistência filho.
3. Selecione ⋮ ; em seguida, selecione **mover sob grupo de consistência diferente**.
4. Insira um novo nome para o grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione o grupo de consistência existente que você gostaria de fazer o grupo de consistência pai ou selecione para criar um novo grupo de consistência pai.

   Se você selecionar criar um novo grupo de consistência pai, digite um nome para o grupo de consistência pai ou aceite o nome padrão; em seguida, selecione o tipo de componente do aplicativo de consistência.

6. Selecione **mover**.

O que vem a seguir

Depois de criar um grupo de consistência filho, você pode"aplicar políticas individuais de proteção de snapshot" para cada grupo de consistência infantil. Você também pode"configurar políticas de replicação" nos grupos de consistência pai e filho para replicar os grupos de consistência em um local remoto.

Separe um grupo de consistência filho de um grupo de consistência pai

Quando você separa um grupo de consistência filho de um grupo de consistência pai, o grupo de consistência filho é removido do grupo de consistência pai e é gerenciado como um único grupo de consistência. A política de replicação aplicada ao pai não é mais aplicada ao grupo de consistência filho desanexado.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja destacar estiver em um relacionamento de sincronização ativo do SnapMirror , você deve"excluir o relacionamento de sincronização ativa do SnapMirror" antes que o grupo de consistência possa ser destacado. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve"romper o relacionamento" antes de poder desanexar o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione o grupo de consistência pai.
3. Selecione sobre o grupo de consistência filho que deseja separar.
4. Selecione ⋮ ; em seguida, selecione **Desanexar do pai**.
5. Insira um novo nome para o grupo de consistência que você está desanexando ou aceite o nome padrão; em seguida, selecione o tipo de aplicativo do grupo de consistência.
6. Selecione **Desanexar**.

O que se segue?

"Configure uma política de replicação"para replicar os instantâneos do grupo de consistência filho desanexado em um cluster remoto.

Gerenciar políticas e programações de proteção de dados da ONTAP em sistemas de storage ASA R2

Use políticas de snapshot para proteger os dados nos grupos de consistência em uma programação automatizada. Use programações de políticas nas políticas de snapshot para determinar com que frequência os snapshots são feitos.

Crie um novo cronograma de política de proteção

Um cronograma de política de proteção define com que frequência uma política de snapshots é executada. Você pode criar programações para serem executadas em intervalos regulares com base em vários dias, horas ou minutos. Por exemplo, você pode criar uma programação para executar a cada hora ou para executar apenas uma vez por dia. Você também pode criar programações para serem executadas em horários específicos em dias específicos da semana ou mês. Por exemplo, você pode criar uma agenda para ser executada às 12:15am no dia 20th de cada mês.

A definição de várias programações de políticas de proteção oferece a flexibilidade de aumentar ou diminuir a frequência de snapshots para diferentes aplicações. Isso permite que você forneça um nível maior de proteção e um risco menor de perda de dados para seus workloads essenciais do que o que pode ser necessário para workloads menos essenciais.

Passos

1. Selecione **proteção > políticas**; em seguida, selecione **Programação**.
2. + Add Selecione .
3. Introduza um nome para a programação e, em seguida, selecione os parâmetros de programação.
4. Selecione **Guardar**.

O que se segue?

Agora que você criou uma nova agenda de políticas, pode usar a programação recém-criada em suas políticas para definir quando os snapshots são feitos.

Criar uma política de snapshot

Uma política de snapshot define com que frequência os snapshots são feitos, o número máximo de snapshots permitidos e o tempo de retenção dos snapshots.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2. + Add Selecione .
3. Introduza um nome para a política de instantâneos.
4. Selecione **Cluster** para aplicar a política a todo o cluster. Selecione **Storage VM** para aplicar a política a uma VM de armazenamento individual.
5. Selecione **Adicionar um agendamento**; em seguida, insira o agendamento da política de snapshot.
6. Selecione **Adicionar política**.

O que se segue?

Agora que você criou uma política de snapshot, pode aplicá-la a um grupo de consistência. Os instantâneos serão tirados do grupo de consistência com base nos parâmetros definidos na política de instantâneos.

Aplique uma política de snapshot a um grupo de consistência

Aplique uma política de snapshot a um grupo de consistência para criar, reter e rotular automaticamente snapshots do grupo de consistência.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2. Passe o Mouse sobre o nome da política de snapshot que você deseja aplicar.
3. ⋮ Selecione ; em seguida, selecione **aplicar**.
4. Selecione os grupos de consistência aos quais você deseja aplicar a política de snapshot; em seguida, selecione **aplicar**.

O que se segue?

Agora que seus dados estão protegidos com snapshots, você deve "configure uma relação de replicação"copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Edite, exclua ou desative uma política de snapshot

Edite uma política de instantâneos para modificar o nome da política, o número máximo de instantâneos ou o rótulo SnapMirror. Exclua uma política para removê-la e seus dados de backup associados do cluster.

Desative uma política para interromper temporariamente a criação ou transferência de instantâneos especificados pela política.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2. Passe o Mouse sobre o nome da política de snapshot que você deseja editar.
3. Selecione ⋮; em seguida, selecione **Edit**, **Delete** ou **Disable**.

Resultado

Você modificou, excluiu ou desativou a política de snapshot.

Editar uma política de replicação

Edite uma política de replicação para modificar a descrição da política, o agendamento de transferência e as regras. Também pode editar a política para ativar ou desativar a compressão de rede.

Passos

1. No System Manager, selecione **proteção > políticas**.
2. Selecione **políticas de replicação**.
3. Passe o Mouse sobre a política de replicação que você deseja editar; em seguida, ⋮selecione .
4. Selecione **Editar**.
5. Atualize a política; em seguida, selecione **Salvar**.

Resultado

Você modificou a política de replicação.

Proteja seus dados

Criptografia de dados em repouso em sistemas de storage ASA R2

Ao criptografar dados em repouso, não é possível ler se um meio de storage é reutilizado, devolvido, extraviado ou roubado. Você pode usar o Gerenciador de sistemas do ONTAP para criptografar seus dados em nível de hardware e software para proteção de camada dupla.

O NetApp Storage Encryption (NSE) é compatível com a criptografia de hardware usando unidades de autocriptografia (SEDs). Os SEDs criptografam dados conforme são gravados. Cada SED contém uma chave de criptografia exclusiva. Os dados criptografados armazenados no SED não podem ser lidos sem a chave de criptografia do SED. Os nós que tentam ler de um SED devem ser autenticados para acessar a chave de criptografia do SED. Os nós são autenticados pela obtenção de uma chave de autenticação de um gerenciador de chaves e, em seguida, apresentando a chave de autenticação à SED. Se a chave de autenticação for válida, o SED dará ao nó a sua chave de encriptação para aceder aos dados que contém.

ⓘ Nos sistemas ASA r2, os SEDs são suportados apenas para SSDs baseados em NVMe.

Use o gerenciador de chaves integrado do ASA R2 ou um gerenciador de chaves externo para fornecer chaves de autenticação aos nós.

Além do NSE, você também pode habilitar a criptografia de software para adicionar outra camada de

segurança aos seus dados.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, em **criptografia**, selecione **Configurar**.
3. Configure o gerenciador de chaves.

Opção	Passos
Configure o Onboard Key Manager	a. Selecione **Onboard Key Manager** para adicionar os servidores de chave. b. Introduza uma frase-passe.
Configurar um gerenciador de chaves externo	a. Selecione **Gerenciador de chaves externo** para adicionar os servidores de chaves. b. + Add Selecione para adicionar os servidores de chaves. c. Adicione os certificados de CA do servidor KMIP. d. Adicione os certificados de cliente KMIP.

4. Selecione **encriptação de camada dupla** para ativar a encriptação de software.
5. Selecione **Guardar**.

O que se segue?

Agora que você criptografou seus dados em repouso, se estiver usando o protocolo NVMe/TCP, poderá "criptografe todos os dados enviados pela rede" entre o host NVMe/TCP e o sistema ASA R2.

Migre chaves de criptografia de dados ONTAP entre gerenciadores de chaves no sistema ASA R2

Você pode gerenciar suas chaves de criptografia de dados usando o Gerenciador de chaves integrado do ONTAP no sistema ASA R2 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 no nível de VM de armazenamento	Apenas um gerenciador de chaves externo

Se ativar o seu gestor de chaves na…	Você pode usar…
Tanto no nível do cluster quanto no nível da VM de armazenamento	Uma das seguintes combinações de gerenciador de chaves: • Opção 1 Nível de cluster: Gerenciador de chaves integrado Nível de VM de armazenamento: Gerenciador de chaves externo • Opção 2 Nível de cluster: Gerenciador de chaves externo Nível de VM de armazenamento: Gerenciador 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.

De bordo para 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 <storage_vm_name>
-type KMIP
```

4. Exclua a configuração do gerenciador de chaves integrado:

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Do externo ao 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 <storage_vm_name>
-type OKM
```

4. Exclua a configuração do gerenciador de chaves externo

```
security key-manager keystore delete-config -vserver
<storage_vm_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 <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Proteção contra ataques de ransomware

Crie instantâneos à prova de violação para proteger contra ataques de ransomware em sistemas de armazenamento ASA r2

Para maior proteção contra ataques de ransomware, replique snapshots para um cluster remoto e bloqueie os snapshots de destino para torná-los à prova de violação. Os instantâneos bloqueados não podem ser eliminados acidentalmente ou maliciosamente. Use snapshots bloqueados para recuperar dados caso uma unidade de storage seja

comprometida por um ataque de ransomware.

Inicialize o relógio SnapLock Compliance

Antes de criar snapshots à prova de adulteração, é necessário inicializar o relógio SnapLock Compliance nos clusters local e de destino.

Passos

1. Selecione **Cluster > Overview**.
2. Na seção **nós**, selecione **Inicializar Relógio SnapLock Compliance**.
3. Selecione **Inicializar**.
4. Verifique se o relógio de conformidade foi inicializado.
   a. Selecione **Cluster > Overview**.
   b. Na seção **nós**, selecione ; em seguida, selecione **Relógio SnapLock Compliance**.

O que vem a seguir?

Depois de inicializar o relógio SnapLock Compliance nos clusters local e de destino, você estará pronto para "crie uma relação de replicação com instantâneos bloqueados".

Habilite a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. A ARP/AI detecta rapidamente potenciais ameaças de ransomware, cria automaticamente um snapshot da ARP para proteger seus dados e exibe uma mensagem de aviso no Gerenciador do Sistema para alertá-lo sobre atividades suspeitas.

O ARP aprimora a resiliência cibernética ao adotar um modelo de aprendizado de máquina para análise antiransomware que detecta formas de ransomware em constante evolução com 98% de precisão em ambientes SAN. O modelo de aprendizado de máquina do ARP é pré-treinado em um grande conjunto de dados de arquivos, tanto antes quanto depois de um ataque de ransomware simulado. Esse treinamento que exige muitos recursos é realizado fora do ONTAP, e o modelo pré-treinado resultante desse treinamento é incluído on-box com o ONTAP. Esse modelo não é acessível nem modificável. O ARP/AI é ativado imediatamente após a capacitação; não há "período de aprendizagem".

> Nenhum sistema de detecção ou prevenção de ransomware pode garantir completamente a segurança contra um ataque de ransomware. Embora um ataque possa passar despercebido, ARP/AI atua como uma importante camada adicional de defesa caso o software antivírus falhe em detectar uma intrusão.

Sobre esta tarefa

- O suporte ARP/AI está incluído no "Licença ONTAP One" .
- ARP/AI não é compatível com unidades de armazenamento protegidas por SnapMirror active sync, SnapMirror synchronous ou SnapLock.
- A partir do ONTAP 9.18.1, o ARP/AI é ativado por padrão em todas as unidades de armazenamento recém-criadas 12 horas após a atualização para o ONTAP 9.18.1 ou a inicialização de um novo cluster ASA r2 com ONTAP 9.18.1.
- Depois de habilitar o ARP/AI, você deve "habilite atualizações automáticas para seus arquivos de

segurança" para receber automaticamente novas atualizações de segurança.

Ative o ARP/AI em todas as unidades de armazenamento no cluster

Se você estiver executando ONTAP 9.17.1, você pode habilitar ARP/AI em todas as unidades de armazenamento criadas no cluster por padrão.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Anti-ransomware**, selecione ⋮ e, em seguida, selecione **Ativar em todas as unidades de armazenamento existentes**.
3. Selecione **Ativar**.

Habilite ARP/AI em todas as unidades de armazenamento em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1, poderá habilitar ARP/AI em todas as unidades de armazenamento criadas em uma máquina virtual de armazenamento (VM) por padrão. Isso significa que qualquer nova unidade de armazenamento criada na máquina virtual de armazenamento terá ARP/AI habilitado automaticamente. Você também pode aplicar ARP/AI a unidades de armazenamento existentes na máquina virtual de armazenamento.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No Gerenciador do Sistema, selecione **Cluster > VMs de Armazenamento**.
2. Selecione a VM de armazenamento na qual você deseja habilitar o ARP/AI.
3. Na seção **Segurança**, ao lado de **Anti-ransomware**, selecione ⋮ ; então selecione **Editar configurações anti-ransomware**.
4. Selecione **Ativar anti-ransomware**.

   Isso habilita ARP/AI em todas as futuras unidades de armazenamento criadas na VM de armazenamento selecionada por padrão.

5. Para aplicar o ARP às unidades de armazenamento existentes na VM de armazenamento selecionada, selecione **Aplicar esta alteração a todas as unidades de armazenamento existentes aplicáveis nesta VM de armazenamento**.
6. Selecione **Guardar**.

Resultado

Todas as novas unidades de armazenamento que você criar na máquina virtual de armazenamento são protegidas contra ataques de ransomware por padrão, e qualquer atividade suspeita será relatada a você no Gerenciador de Sistemas.

Habilite ARP/AI em unidades de armazenamento específicas em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1 e não quiser que ARP/AI esteja habilitado em todas as unidades de armazenamento em uma storage VM, você pode selecionar as unidades específicas que deseja habilitar.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja habilitar ARP/AI.
3. Selecione ⋮ ; então selecione **Ativar anti-ransomware**.
4. Selecione **Ativar**.

Resultado

As unidades de armazenamento selecionadas são protegidas contra ataques de ransomware, e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Desative a proteção autônoma padrão contra ransomware em seus sistemas de armazenamento ASA r2

Ao inicializar um novo cluster ONTAP 9.18.1 ASA r2 ou ao atualizar seu cluster para ONTAP 9.18.1, o ARP/AI é ativado automaticamente por padrão em todas as novas unidades de armazenamento após um período de carência de 12 horas. Se você não desativar o ARP/AI durante o período de carência, ele será ativado em todo o cluster para as novas unidades de armazenamento quando o período de carência terminar.

As unidades de armazenamento criadas no ONTAP 9.17.1 devem ser "ativado manualmente" para ARP/AI.

Passos

Você pode desativar a capacitação padrão durante ou após o período de carência inicial de 12 horas.

System Manager

1. Selecione **Cluster > Settings**.
2. Desativar ARP:
   - Para desativar durante o período de carência de 12 horas:
     i. Em **Anti-ransomware**, selecione **Don't enable** e depois selecione **Disable**.
   - Para desativar após o período de carência de 12 horas:
     i. Em **Anti-ransomware**, selecione e desmarque **Ativar para novas unidades de armazenamento**.
     ii. Selecione **Save**

CLI

1. Verifique o status de capacitação padrão:

```
security anti-ransomware auto-enable show
```

2. Desative a capacitação padrão para volumes existentes e novos:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modificar períodos de retenção de snapshots ARP/AI em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, ela criará automaticamente um snapshot ARP para proteger os dados da unidade de armazenamento. Dependendo da sua capacidade de armazenamento e dos requisitos de negócios para seus dados, você pode aumentar ou diminuir o período de retenção padrão do snapshot ARP. Por exemplo, você pode aumentar o período de retenção para aplicativos críticos para os negócios, de modo que, se necessário, tenha períodos de retenção mais longos para recuperação de dados, ou pode diminuir o período de retenção para aplicativos não críticos, economizando espaço de armazenamento.

O período de retenção padrão para o snapshot do ARP varia dependendo da ação que você toma em resposta à atividade anormal.

Se você tomar essa atitude…	Os instantâneos ARP são retidos por padrão para…
Marcar como falso positivo	12 horas
Marcar como potencial ataque de ransomware	7 dias

Se você tomar essa atitude…	Os instantâneos ARP são retidos por padrão para…
Não tome medidas imediatas	10 dias

Os períodos de retenção padrão podem ser modificados usando a interface de linha de comando (CLI) do ONTAP . Veja "Modificar opções para snapshots automáticos do ONTAP" para saber as etapas para alterar o período de retenção padrão.

Responda à proteção autônoma contra ransomware com alertas de IA em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, um aviso será gerado no painel do Gerenciador de Sistemas. Você deve visualizar o aviso, verificar a atividade e, se necessário, tomar medidas para impedir qualquer ameaça potencial aos seus dados.

Se uma mensagem de aviso ARP/AI for exibida, antes de tomar qualquer medida, você deve usar o verificador de integridade do aplicativo apropriado para verificar a integridade dos dados na unidade de armazenamento. Verificar a integridade dos dados da unidade de armazenamento ajuda a determinar se a atividade é aceitável ou se se trata de um possível ataque de ransomware.

Se a atividade anormal for …	Então faça isto…
Aceitável	Marque a atividade como um falso positivo.
Um potencial ataque de ransomware	Marque a atividade como um possível ataque de ransomware.
Indeterminado	Não tome medidas imediatas. Monitore a unidade de armazenamento por até 7 dias. Se a unidade de armazenamento continuar operando normalmente, marque a atividade como um falso positivo. Se a unidade de armazenamento continuar apresentando atividade anormal, marque a atividade como um possível ataque de ransomware.

Passos

1. No System Manager, selecione **Dashboard**.

   Se o ARP detectar atividade anormal em uma ou mais unidades de armazenamento, uma mensagem será exibida em **Avisos**.

2. Selecione a mensagem de aviso.
3. Em **Visão geral de eventos**, selecione a mensagem **Avisos** que indica o número de unidades de armazenamento com atividade anormal.
4. Em **Unidades de armazenamento com atividade anormal**, selecione a unidade de armazenamento.
5. Selecione **Segurança**.

   Se houver atividade anormal na unidade de armazenamento, uma mensagem será exibida em **Anti-ransomware**.

6. Selecione **Escolher uma ação**.
7. Selecione **Marcar como falso positivo** ou selecione **Marcar como possível ataque de ransomware**.

O que se segue?

Se você observar picos na atividade de suas unidades de armazenamento, sejam eles pontuais ou característicos de um novo padrão, você deve reportá-los como seguros. Reportar esses picos manualmente como seguros ajuda a melhorar a precisão das avaliações de ameaças do ARP. Saiba como "relatar picos conhecidos de ARP/AI".

Pause ou retome a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. Se estiver planejando um evento de carga de trabalho incomum, você pode suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware. Após a conclusão do evento de carga de trabalho, você pode retomar a análise de ARP/AI.

Pausar ARP/AI

Antes de iniciar um evento de carga de trabalho incomum, pode ser necessário suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja pausar o ARP/AI.
3. Selecione **Pausar anti-ransomware**.

Resultado

A análise de ARP/AI é pausada para as unidades de armazenamento selecionadas, e nenhuma atividade suspeita é relatada a você no Gerenciador do Sistema até que você retome o ARP/AI.

Retomar ARP/AI

Se você pausar o ARP/AI durante uma carga de trabalho incomum, após a conclusão da carga de trabalho, você deverá retomá-la para proteger seus dados contra ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja retomar o ARP/AI.
3. Selecione **Retomar anti-ransomware**.

Resultado

A análise de potenciais ataques de ransomware é retomada e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Conexões NVMe seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo NVMe, poderá configurar a autenticação na banda para aprimorar a segurança dos dados. A autenticação na banda permite autenticação bidirecional e unidirecional segura entre os hosts NVMe e o sistema ASA R2. A autenticação na banda está disponível para todos os hosts NVMe. Se você estiver usando o protocolo NVMe/TCP, poderá aprimorar ainda mais a segurança dos dados configurando a segurança da camada de transporte (TLS) para criptografar todos os dados enviados pela rede entre os hosts NVMe/TCP e o sistema ASA R2.

Passos

1. Selecione **hosts**; em seguida, selecione **NVMe**.
2. 

Selecione .
3. Insira o nome do host e selecione o sistema operacional do host.
4. Insira uma descrição do host; em seguida, selecione a VM de armazenamento a ser conetada ao host.
5. Selecione ao lado do nome do host.
6. Selecione **Autenticação na banda**.
7. Se você estiver usando o protocolo NVMe/TCP, selecione **exigir segurança da camada de transporte (TLS)**.
8. Selecione **Adicionar**.

Resultado

A segurança dos seus dados é melhorada com autenticação na banda e/ou TLS.

Conexões IP seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo IP no sistema ASA R2, poderá configurar a segurança IP (IPsec) para melhorar a segurança dos dados. O IPsec é um padrão da Internet que fornece criptografia de dados em trânsito, autenticação para o tráfego que flui entre os pontos de extremidade da rede em um nível IP e proteção contra repetição e ataques mal-intencionados contra seus dados.

Para sistemas ASA R2, o IPsec está disponível para hosts iSCSI e NVMe/TCP.

Em determinados sistemas ASA R2, várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa de controlador de interface de rede (NIC) suportada. A taxa de transferência para operações descarregadas para a placa NIC é de aproximadamente 5% ou menos. Isso pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido pelo IPsec.

A partir do ONTAP 9.18.1, o suporte para descarregamento de hardware IPsec foi estendido ao tráfego IPv6.

As seguintes placas de rede são compatíveis com o descarregamento de hardware nos seguintes sistemas ASA r2 e versões do ONTAP :

Placa NIC suportada	Sistemas ASA r2	Versão ONTAP
X50135A (Controlador Ethernet 2p, 40G/100G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 e posterior
X60135A (Controlador Ethernet 2p, 40G/100G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 e posterior
X50131A - (controlador Ethernet 2P, 40G/100g/200g/400G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 e posterior
X60132A - (controlador Ethernet 4P, 10G/25G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 e posterior

Veja o"NetApp Hardware Universe" Para obter mais informações sobre os sistemas e placas suportados.

O que se segue?

O IPsec é configurado no seu sistema ASA r2 da mesma forma que em outros sistemas ONTAP . Para mais informações, consulte "Prepare-se para configurar a segurança IP para a rede ONTAP.".

Administrar e monitorar

Atualizar e reverter o ONTAP

Atualizar o ONTAP em sistemas de storage ASA R2

Ao atualizar o software ONTAP no sistema ASA R2, você pode aproveitar os novos e aprimorados recursos do ONTAP que ajudam a reduzir custos, acelerar workloads críticos, melhorar a segurança e expandir o escopo de proteção de dados disponível para sua organização.

As atualizações de software da ONTAP para sistemas ASA R2 seguem o mesmo processo que as atualizações para outros sistemas ONTAP. Se você tiver um contrato SupportEdge ativo para o consultor digital da Active IQ (também conhecido como consultor digital), você deve "Prepare-se para atualizar com o Upgrade Advisor". O Upgrade Advisor fornece inteligência que ajuda você a minimizar a incerteza e o risco, avaliando seu cluster e criando um plano de atualização específico para sua configuração. Se você não tiver um contrato SupportEdge ativo para o consultor digital da Active IQ, você deve "Prepare-se para atualizar sem o Upgrade Advisor".

Depois de se preparar para a atualização, é recomendável que você execute atualizações usando "Atualização automatizada e sem interrupções (ANDU) do System Manager"o . O ANDU aproveita a tecnologia de failover de alta disponibilidade (HA) da ONTAP para garantir que os clusters continuem fornecendo dados sem interrupção durante a atualização.

Saiba mais "Atualizações de software ONTAP"sobre o .

Reverter ONTAP em sistemas de armazenamento ASA r2

As reversões de software ONTAP para sistemas ASA r2 seguem o mesmo processo de reversões para outros sistemas ONTAP .

A reversão de um cluster ONTAP é disruptiva. Você deve deixar o cluster offline durante a reversão. Você não deve reverter um cluster de produção sem assistência do suporte técnico. Você pode reverter um cluster novo ou de teste sem assistência. Se a reversão de um sistema novo ou de teste falhar ou for concluída com sucesso, mas você não estiver satisfeito com o desempenho do cluster em seu ambiente de produção, entre em contato com o suporte técnico para obter assistência.

"Reverter um cluster ONTAP" .

Rever requisitos para sistemas ASA r2

Certas configurações de cluster ASA r2 exigem que você execute ações específicas antes de iniciar uma reversão de software ONTAP .

Revertendo do ONTAP 9.17.1

Se você estiver revertendo do ONTAP 9.17.1 em um sistema ASA r2, execute as seguintes ações antes de iniciar a reversão:

"equilíbrio espacial dinâmico"É ativado por padrão 14 dias após a atualização para o ONTAP 9.17.1 ou a inicialização de um novo cluster ONTAP 9.17.1 ASA r2. Não é possível reverter do ONTAP 9.17.1 para o ASA r2 após a ativação do balanceamento dinâmico de espaço.

Se você tem…	Antes de reverter você deve…
Grupos de consistência hierárquica em um relacionamento de sincronização ativa do SnapMirror	"Excluir o relacionamento de sincronização ativa do SnapMirror".
Relacionamentos de importação ativos	Exclua os relacionamentos de importação ativos. "Saiba mais sobre relações de importação".
Proteção anti-ransomware habilitada	"Desative a proteção contra ransomware.".

Atualize o firmware em sistemas de armazenamento ASA R2

O ONTAP transfere e atualiza automaticamente ficheiros de firmware e de sistema no seu sistema ASA R2 por predefinição. Se você quiser a flexibilidade de visualizar as atualizações recomendadas antes que elas sejam baixadas e instaladas, você pode usar o Gerenciador de sistema do ONTAP para desativar atualizações automatizadas ou editar parâmetros de atualização para mostrar notificações de atualizações disponíveis antes que qualquer ação seja executada.

Ativar atualizações automáticas

As atualizações recomendadas para firmware de armazenamento, firmware SP/BMC e ficheiros de sistema são automaticamente transferidas e instaladas no sistema ASA R2 por predefinição. Se as atualizações automáticas tiverem sido desativadas, você poderá habilitá-las a restabelecer o comportamento padrão.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Atualizações de software**, selecione **Ativar**.
3. Leia o CLUF.
4. Aceite os padrões para **Mostrar notificação** de atualizações recomendadas. Opcionalmente, selecione **Atualizar automaticamente** ou **Descartar automaticamente** as atualizações recomendadas.
5. Selecione para confirmar que suas modificações de atualização serão aplicadas a todas as atualizações atuais e futuras.
6. Selecione **Guardar**.

Resultado

As atualizações recomendadas são transferidas e instaladas automaticamente no sistema ASA R2 com base nas seleções de atualização.

Desativar as atualizações automáticas

Desative as atualizações automáticas somente se você quiser gerenciar as atualizações inteiramente por conta própria. Com as atualizações automáticas desativadas, o sistema não notificará, baixará ou instalará atualizações. Você é responsável por monitorar, baixar, agendar e instalar todas as atualizações manualmente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Atualizações de software**, selecione **Desativar**.

Resultado

As atualizações automáticas estão desativadas. Deve verificar regularmente as atualizações recomendadas e decidir se pretende efetuar uma instalação manual.

Ver atualizações automáticas

Veja uma lista de atualizações de firmware e de ficheiros de sistema que foram transferidas para o cluster e que estão agendadas para instalação automática. Veja também as atualizações que foram instaladas automaticamente anteriormente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Atualizações de software** selecione → e selecione **Exibir todas as atualizações automáticas**.

Editar atualizações automáticas

Você pode optar por ter as atualizações recomendadas para o firmware de armazenamento, o firmware SP/BMC e os arquivos de sistema baixados e instalados automaticamente no cluster, ou pode optar por ter as atualizações recomendadas descartadas automaticamente. Se você quiser controlar manualmente a instalação ou a demissão de atualizações, selecione para ser notificado quando uma atualização recomendada estiver disponível; então você pode selecionar manualmente para instalá-la ou descartá-la.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Atualizações de software** selecione → e selecione **Todas as outras atualizações**.
3. Atualize as seleções para atualizações automáticas.
4. Selecione **Guardar**.

Resultado

As atualizações automáticas são modificadas com base nas suas seleções.

Atualize o firmware manualmente

Se você quiser a flexibilidade de visualizar as atualizações recomendadas antes que elas sejam baixadas e instaladas, você pode desativar as atualizações automatizadas e atualizar seu firmware manualmente.

Passos

1. Transfira o ficheiro de atualização do firmware para um servidor ou cliente local.
2. No Gerenciador do Sistema, selecione **Cluster > Visão geral** e, em seguida, selecione **Todas as outras atualizações**.
3. Em **Atualizações manuais**, selecione **Adicionar arquivos de firmware**; depois selecione **Baixar do servidor** ou **Carregar do cliente local**.
4. Instale o arquivo de atualização de firmware.

Resultado

O firmware é atualizado.

Gerenciar o acesso do cliente a VMs de storage em sistemas de storage ASA R2

As unidades de armazenamento em um sistema ASA R2 estão contidas nas máquinas virtuais de armazenamento (VMs). As VMs de storage são usadas para fornecer dados aos clientes de SAN. Use o Gerenciador do sistema ONTAP para criar um LIF (interface de rede) para que seus clientes SAN se conetem a uma VM de storage e acessem dados nas unidades de armazenamento. Opcionalmente, você pode usar sub-redes para simplificar a criação de LIF e IPspaces para fornecer às VMs de armazenamento seu próprio armazenamento seguro, administração e roteamento.

Crie uma VM de storage

Durante a configuração do cluster, sua máquina virtual de armazenamento de dados (VM) padrão é criada. Todas as novas unidades de armazenamento são criadas dentro da VM de armazenamento de dados padrão, a menos que você crie e selecione uma VM de armazenamento diferente. Você pode criar uma VM de armazenamento adicional para segregar suas unidades de armazenamento para diferentes aplicativos, departamentos ou clientes. Por exemplo, você pode querer criar uma VM de storage para seu ambiente de desenvolvimento e outra VM de storage para seu ambiente de produção ou criar uma VM de storage para seu departamento financeiro e outra VM de storage para seu departamento de marketing.

Passos

1. Selecione **Cluster > Storage VMs**.
2. + Add Selecione .
3. Insira um nome para a VM de armazenamento ou aceite o nome padrão.
4. Em **Configurar protocolos**, selecione os protocolos para a VM de armazenamento.

   Selecione **IP** para iSCSI e NVMe/TCP. Selecione **FC** para Fibre Channel ou NVMe/FC.

5. Em **Storage VM Administration**, selecione **Manage administrator account** (gerir conta de administrador); em seguida, introduza o nome de utilizador e a palavra-passe da conta de administrador.
6. Adicione uma interface de rede para a VM de storage.
7. Selecione **Guardar**.

O que se segue?

Você criou uma VM de storage. Agora você pode usar a VM de storage para "provisionamento de storage".

Crie IPspaces

Um espaço IPspace é um espaço de endereço IP distinto no qual as VMs de armazenamento residem. Quando você cria IPspaces, você habilita as VMs de armazenamento para ter seu próprio armazenamento seguro, administração e roteamento. Você também permite que os clientes em domínios de rede separados administrativamente usem endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Você deve criar um espaço IPspace antes de criar uma sub-rede.

Passos

1. Selecione **rede > Visão geral**.
2. Em **IPspaces**, + Add selecione .
3. Introduza um nome para o IPspace ou aceite o nome predefinido.

   Um nome IPspace não pode ser "All" porque "All" é um nome reservado ao sistema.

4. Selecione **Guardar**.

O que se segue?

Agora que você criou um espaço IPspace, você pode usá-lo para criar uma sub-rede.

Crie sub-redes

Uma sub-rede permite alocar blocos específicos de endereços IPv4 ou IPv6 para usar quando você cria um LIF (interface de rede) . Uma sub-rede simplifica a criação de LIF, permitindo que você especifique o nome da sub-rede em vez de um endereço IP específico e uma máscara de rede para cada LIF.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- O "domínio de transmissão" e o espaço IPspace onde pretende adicionar a sub-rede já devem existir.

Passos

1. Selecione **rede > Visão geral**.
2. Selecione **sub-redes**; em seguida, + Add selecione .
3. Introduza o nome da sub-rede.

   Todos os nomes de sub-rede devem ser exclusivos dentro de um espaço IPspace.

4. Introduza o endereço IP da sub-rede e a máscara de sub-rede.
5. Especifique o intervalo de endereços IP para a sub-rede.

   Quando especificar o intervalo de endereços IP para a sub-rede, não sobreponha endereços IP com outras sub-redes. Problemas de rede podem ocorrer quando os endereços IP de sub-rede se sobrepõem e diferentes sub-redes ou hosts tentam usar o mesmo endereço IP.

6. Selecione o domínio de broadcast para a sub-rede.
7. Selecione **Adicionar**.

O que se segue?

Você criou uma sub-rede que agora pode usar para simplificar a criação de seus LIFs.

Criar um LIF (interface de rede)

Um LIF (interface de rede) é um endereço IP associado a uma porta física ou lógica. Crie LIFs nas portas que você deseja usar para acessar dados. As VMs de storage fornecem dados aos clientes por meio de uma ou mais LIFs. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, de modo que a comunicação de rede não seja interrompida.

Em um sistema ASA R2, você pode criar LIFs IP, FC e NVMe/FC. Um LIF de dados IP pode atender o tráfego iSCSI e NVMe/TCP por padrão. É necessário criar LIFs de dados separados para o tráfego FC e NVMe/FC.

Se pretender ativar o failover de LIF iSCSI automático, tem de criar um LIF IP para tráfego apenas iSCSI. Quando o failover automático de LIF iSCSI é ativado, se ocorrer um failover de armazenamento, o IP iSCSI LIF é migrado automaticamente de seu nó ou porta inicial para seu nó ou porta parceiro de HA e, em seguida, volta assim que o failover for concluído. Ou, se a porta para um IP iSCSI LIF não for saudável, o LIF é migrado automaticamente para uma porta saudável em seu nó inicial atual e, em seguida, de volta para sua porta original quando a porta estiver funcionando novamente.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.
- Um tráfego entre nós que lida com LIF não deve estar na mesma sub-rede que um tráfego de gerenciamento de manipulação de LIF ou um tráfego de dados de manipulação de LIF.

Passos

1. Selecione **rede > Visão geral**.
2. Selecione **interfaces de rede**; em seguida, + Add selecione .
3. Selecione o tipo de interface e o protocolo e, em seguida, selecione a VM de armazenamento.
4. Introduza um nome para o LIF ou aceite o nome predefinido.
5. Selecione o nó inicial para a interface de rede e, em seguida, introduza o endereço IP e a máscara de sub-rede.
6. Selecione **Guardar**.

Resultado

Você criou um LIF para acesso aos dados.

O que se segue?

Você pode usar a interface de linha de comando (CLI) do ONTAP para criar um LIF somente iSCSI com failover automático.

Crie uma política de serviço LIF personalizada somente iSCSI

Se você quiser criar LIFs somente iSCSI com failover automático de LIF, primeiro crie uma política de serviço LIF somente iSCSI personalizada.

Você deve usar a interface de linha de comando (CLI) do ONTAP para criar a política de serviço personalizada.

Passo

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Crie uma política de serviço LIF personalizada somente para iSCSI:

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. Verifique se a política de serviço foi criada:

```
network interface service-policy show -policy <service_policy_name>
```

4. Retorne o nível de privilégio para admin:

```
set -privilege admin
```

Crie LIFs somente iSCSI com failover automático de LIF

Se existirem LIFs iSCSI na VM de armazenamento que não estejam habilitadas para failover automático de LIF, as LIFs recém-criadas também não serão habilitadas para failover automático de LIF. Se o failover automático de LIF não estiver habilitado e ocorrer um evento de failover, suas LIFs iSCSI não serão migradas.

Antes de começar

Você deve ter criado uma política de serviço LIF personalizada somente iSCSI.

Passos

1. Crie LIFs somente iSCSI com failover automático de LIF:

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

   - Recomenda-se criar dois iSCSI LIFs em cada nó, um para a malha A e outro para a malha B. Isso proporciona redundância e balanceamento de carga para o tráfego iSCSI. No exemplo a seguir, são criados um total de quatro iSCSI LIFs, dois em cada nó e um para cada malha.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- Se você estiver usando VLANs, ajuste o `home-port` parâmetro para incluir as informações da porta VLAN para a respectiva estrutura iSCSI, por exemplo, `-home-port e2b-<iSCSI-A-VLAN>` para tecido iSCSI A e `-home-port e4b-<iSCSI-B-VLAN>` .
- Se você estiver usando grupos de interface (ifgroups) com VLANs, ajuste o `home-port` parâmetro para incluir a porta VLAN apropriada, por exemplo, `-home-port a0a-<iSCSI-A-VLAN>` para tecido iSCSI A e `-home-port a0a-<iSCSI-B-VLAN>` para tecido iSCSI B onde `a0a` é o ifgroup e a0a-<iSCSI-A-VLAN> e a0a-<iSCSI-B-VLAN> são as respectivas portas VLAN para a estrutura iSCSI A e a estrutura iSCSI B.

2. Verifique se os LIFs iSCSI foram criados:

```
network interface show -lif iscsi*
```

Modificar um LIF (interfaces de rede)

Os LIFs podem ser desativados ou renomeados conforme necessário. Você também pode alterar o endereço IP de LIF e a máscara de sub-rede.

Sobre esta tarefa

O ONTAP utiliza o Network Time Protocol (NTP) para sincronizar o tempo no cluster. Após alterar os endereços IP do LIF, talvez seja necessário atualizar a configuração do NTP para evitar falhas de sincronização. Para obter mais informações, consulte o artigo da Base de Conhecimento"A sincronização NTP falha após a alteração do IP do LIF" .

Passos

1. Selecione **rede > Visão geral**; em seguida, selecione **interfaces de rede**.

2. Passe o Mouse sobre a interface de rede que você deseja editar; em seguida, selecione .
3. Selecione **Editar**.
4. Pode desativar a interface de rede, mudar o nome da interface de rede, alterar o endereço IP ou alterar a máscara de sub-rede.
5. Selecione **Guardar**.

Resultado

Seu LIF foi modificado.

Gerenciar a rede de cluster em sistemas de storage ASA R2

Você pode usar o Gerenciador de sistema do ONTAP para executar a administração básica da rede de storage no sistema ASA R2. Por exemplo, você pode adicionar um domínio de broadcast ou reatribuir portas a um domínio de broadcast diferente.

Adicione um domínio de broadcast

Use domínios de broadcast para simplificar o gerenciamento da rede de cluster agrupando portas de rede que pertencem à mesma rede de camada 2. As máquinas virtuais de armazenamento (VMs) podem então usar as portas do grupo para tráfego de dados ou gerenciamento.

O domínio de broadcast "padrão" e o domínio de broadcast "Cluster" são criados durante a configuração do cluster. O domínio de broadcast "padrão" contém portas que estão no IPspace "padrão". Essas portas são usadas principalmente para fornecer dados. As portas de gerenciamento de clusters e de nós também estão neste domínio de transmissão. O domínio de broadcast "Cluster" contém portas que estão no espaço IPspace "Cluster". Essas portas são usadas para comunicação de cluster e incluem todas as portas de cluster de todos os nós no cluster.

Você pode criar domínios de broadcast adicionais após o cluster ter sido inicializado. Quando você cria um domínio de broadcast, um grupo de failover que contém as mesmas portas é criado automaticamente.

Sobre esta tarefa

A unidade máxima de transmissão (MTU) das portas adicionadas a um domínio de broadcast são atualizadas para o valor MTU definido no domínio de broadcast.

Passos

1. No System Manager, selecione **rede > Visão geral**.
2. Em domínios **Broadcast**, + Add selecione .
3. Introduza um nome para o domínio de difusão ou aceite o nome predefinido.

   Todos os nomes de domínio de broadcast devem ser exclusivos dentro de um espaço IPspace.

4. Selecione o espaço IPspace para o domínio de broadcast.

   Se você não especificar um nome de IPspace, o domínio de broadcast será criado no IPspace "padrão".

5. Introduza a unidade de transmissão máxima (MTU).

   MTU é o maior pacote de dados que pode ser aceito no seu domínio de broadcast.

6. Selecione as portas desejadas; em seguida, selecione **Salvar**.

Resultado

Você adicionou um novo domínio de broadcast.

Reatribuir portas a um domínio de broadcast diferente

As portas podem pertencer a apenas um domínio de broadcast. Se você quiser alterar o domínio de broadcast ao qual uma porta pertence, você precisa reatribuir a porta de seu domínio de broadcast existente a um novo domínio de broadcast.

Passos

1. No System Manager, selecione **rede > Visão geral**.
2. Em **Broadcast Domains**, selecione ao lado do nome de domínio; em seguida, selecione **Edit**.
3. Desmarque as portas Ethernet que você deseja reatribuir a outro domínio.
4. Selecione o domínio de broadcast ao qual deseja reatribuir a porta; em seguida, selecione **Reatribuir**.
5. Selecione **Guardar**.

Resultado

Você reatribuiu portas a um domínio de broadcast diferente.

Crie uma VLAN

Uma VLAN consiste em portas de switch agrupadas em um domínio de broadcast. As VLANs permitem aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na infraestrutura de rede IP.

Antes de começar

Os switches implantados na rede devem estar em conformidade com os padrões IEEE 802,1Q.1X ou ter uma implementação de VLANs específica do fornecedor.

Sobre esta tarefa

- Uma VLAN não pode ser criada em uma porta de grupo de interfaces que não contém portas membro.
- Quando você configura uma VLAN por uma porta pela primeira vez, a porta pode cair, resultando em uma desconexão temporária da rede. As adições subsequentes de VLAN à mesma porta não afetam o estado da porta.
- Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

Passos

1. No System Manager, selecione **rede > portas Ethernet** e, em seguida, + VLAN selecione .
2. Selecione o nó e o domínio de broadcast para a VLAN.
3. Selecione a porta para a VLAN.

   A VLAN não pode ser conetada a uma porta que hospeda um cluster LIF ou a portas atribuídas ao cluster IPspace.

4. Insira um ID de VLAN.

5. Selecione **Guardar**.

Resultado

Você criou uma VLAN para aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na sua infraestrutura de rede IP.

Monitorar o uso e aumentar a capacidade

Monitore o desempenho do cluster e da unidade de armazenamento em sistemas de armazenamento ASA R2

Use o Gerenciador de sistema do ONTAP para monitorar o desempenho geral do cluster e o desempenho de unidades de storage específicas para determinar como a latência, o IOPS e a taxa de transferência estão impactando suas aplicações essenciais aos negócios. O desempenho pode ser monitorado em vários períodos de tempo, variando de uma hora a um ano.

Por exemplo, suponha que um aplicativo crítico esteja com alta latência e baixa taxa de transferência. Quando você visualiza o desempenho do cluster nos últimos cinco dias úteis, observa uma diminuição na performance ao mesmo tempo todos os dias. Use essas informações para determinar se o aplicativo crítico está competindo por recursos de cluster quando um processo não crítico começa a ser executado em segundo plano. Você poderá modificar sua política de QoS para limitar o impacto do workload não crítico nos recursos do sistema e garantir que seu workload crítico atenda aos destinos mínimos de taxa de transferência.

Monitorar o desempenho do cluster

Use métricas de performance do cluster para determinar se você precisa mudar os workloads para minimizar a latência e maximizar o IOPS e a taxa de transferência para suas aplicações essenciais.

Passos

1. No System Manager, selecione **Dashboard**.
2. Em **desempenho**, visualize a latência, IOPS e taxa de transferência do cluster por hora, dia, semana, mês ou ano.
3.  Selecione para transferir os dados de desempenho.

O que se segue?

Use as métricas de performance do cluster para analisar se você precisa modificar suas políticas de QoS ou fazer outros ajustes nos workloads da aplicação para maximizar o desempenho geral do cluster.

Monitore o desempenho da unidade de armazenamento

Use as métricas de desempenho da unidade de storage para determinar o impacto de aplicações específicas na latência, IOPS e taxa de transferência.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione a unidade de armazenamento que pretende monitorizar e, em seguida, selecione **Visão geral**.
3. Em **desempenho**, visualize a latência, IOPS e taxa de transferência da unidade de armazenamento por hora, dia, semana, mês ou ano.

4. Selecione para transferir os dados de desempenho.

O que se segue?

Use as métricas de performance da unidade de storage para analisar se você precisa modificar as políticas de QoS atribuídas às unidades de storage a fim de diminuir a latência e maximizar o IOPS e a taxa de transferência.

Monitorar a utilização de cluster e unidades de storage em sistemas de storage ASA R2

Use o Gerenciador do sistema do ONTAP para monitorar a utilização do storage e garantir que você tenha a capacidade de storage necessária para atender a workloads atuais e futuros.

Monitorar a utilização do cluster

Monitore regularmente a quantidade de storage consumida pelo cluster para garantir que, se necessário, esteja preparado para expandir a capacidade do cluster antes de ficar sem espaço.

Passos

1. No System Manager, selecione **Dashboard**.
2. Em **Capacity**, visualize a quantidade de espaço físico usado e a quantidade de espaço disponível no cluster.

   A taxa de redução de dados representa a quantidade de espaço economizado com a eficiência de storage.

O que se segue?

Se o cluster estiver com pouco espaço ou se não tiver capacidade para atender a uma demanda futura, você deve Planejar "adicionar novas unidades"seu sistema ASA R2 para aumentar a capacidade de storage.

Monitorar a utilização de zona de disponibilidade de storage

Cada par de HA em um sistema ASA R2 usa um pool comum de armazenamento chamado *zona de disponibilidade de armazenamento*. A zona de disponibilidade de storage tem acesso a todos os discos disponíveis no sistema de storage e é visível para ambos os nós do par de HA.

Se você tiver 4 ou mais nós no cluster, poderá visualizar a quantidade de espaço usada pela zona de disponibilidade de storage para cada par de HA. Essa métrica não está disponível para clusters de 2 nós.

Passos

1. No System Manager, selecione **Cluster**; em seguida, selecione **Overview**.

   Um resumo da utilização da zona de disponibilidade de storage é exibido para cada par de HA no cluster.

2. Se você quiser métricas mais detalhadas, selecione uma disponibilidade de armazenamento específica.

   Em **Visão geral**, a capacidade da zona de disponibilidade de armazenamento, a quantidade de espaço usado e a taxa de redução de dados são exibidos.

   Em **unidades de armazenamento** é apresentada uma lista de todas as unidades de armazenamento na

zona de disponibilidade de armazenamento.

O que se segue?

Se sua zona de disponibilidade de storage estiver com pouco espaço, você deverá Planejar "mova as unidades de armazenamento"outra zona de disponibilidade de storage para equilibrar a utilização de storage no cluster.

Monitorar a utilização da unidade de storage

Monitore a quantidade de storage consumida por uma unidade de storage para que você possa aumentar proativamente o tamanho da unidade de storage de acordo com as necessidades da sua empresa.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione a unidade de armazenamento que pretende monitorizar e, em seguida, selecione **Visão geral**.
3. Em **armazenamento**, veja o seguinte:
   - Tamanho da sua unidade de armazenamento
   - Quantidade de espaço usado
   - Relação de redução de dados

     A taxa de redução de dados representa a quantidade de espaço economizado com a eficiência de storage
   - Instantâneo utilizado

     O snapshot usado representa a quantidade de storage usada pelos snapshots.

O que se segue?

Se a sua unidade de armazenamento estiver próxima da capacidade, você deve "modifique a unidade de armazenamento"aumentar seu tamanho.

Aumentar a capacidade de storage em sistemas de storage ASA R2

Adicione unidades a um nó ou gaveta para aumentar a capacidade de storage do sistema ASA R2.

Use o NetApp Hardware Universe para se preparar para a instalação de uma nova unidade

Antes de instalar uma nova unidade em um nó ou chassi, use o NetApp Hardware Universe para confirmar se a unidade que você deseja adicionar é compatível com o seu sistema ASA r2 e para identificar o slot correto para a nova unidade. Os slots corretos para adicionar unidades variam dependendo do modelo do sistema e da versão do ONTAP . Em alguns casos, é necessário adicionar unidades a slots específicos em sequência.

Passos

1. Vá para "NetApp Hardware Universe".
2. Em **Produtos**, selecione suas configurações de hardware.
3. Selecione o seu sistema ASA r2.
4. Selecione sua versão do ONTAP; em seguida, selecione **Mostrar resultados**.

5. Abaixo do gráfico, selecione **clique aqui para ver vistas alternativas**; em seguida, escolha a vista que corresponde à sua configuração.
6. Use a exibição de sua configuração para confirmar se sua nova unidade é suportada e o slot correto para instalação.

Resultado

Você confirmou que sua nova unidade é suportada e você sabe o slot apropriado para instalação.

Instale uma nova unidade no ASA R2

O número mínimo de unidades que você deve adicionar em um único procedimento é seis. Adicionar uma única unidade pode reduzir o desempenho.

Sobre esta tarefa

Você deve repetir as etapas deste procedimento para cada unidade.

Passos

1. Aterre-se corretamente.
2. Remova cuidadosamente a moldura da parte frontal do sistema.
3. Insira a nova unidade no slot correto.
   a. Com o manípulo do excêntrico na posição aberta, utilize as duas mãos para introduzir a nova transmissão.
   b. Prima até a unidade parar.
   c. Feche a pega do came de forma a que a unidade fique totalmente assente no plano intermédio e a pega encaixe no devido lugar.

      Certifique-se de que fecha lentamente a pega do excêntrico de forma a que fique corretamente alinhada com a face da unidade.

4. Verifique se o LED de atividade da unidade (verde) está aceso.
   - SE o LED estiver sólido, a unidade tem energia.
   - Se o LED estiver piscando, a unidade tem energia e e/S está em andamento. O LED também piscará se o firmware da unidade estiver sendo atualizado.

     O firmware da unidade é atualizado automaticamente (sem interrupções) em novas unidades que não tenham versões de firmware atuais.

5. Se o nó estiver configurado para atribuição automática de unidade, você poderá esperar que o ONTAP atribua automaticamente as novas unidades a um nó. Se o nó não estiver configurado para atribuição automática de unidade ou se preferir, você poderá atribuir as unidades manualmente.

   As novas unidades não são reconhecidas até que sejam atribuídas a um nó.

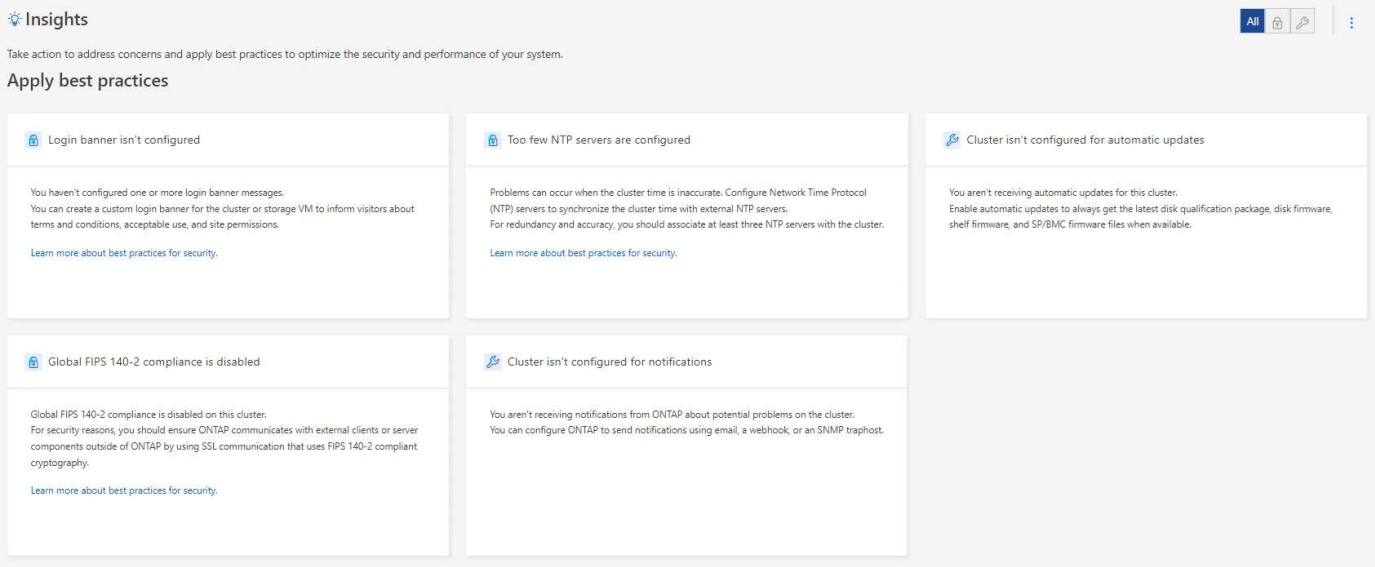
O que vem a seguir?

Depois que as novas unidades tiverem sido reconhecidas, verifique se foram adicionadas e se sua propriedade está especificada corretamente.

Otimize a segurança e a performance do cluster com os insights do sistema de storage do ASA R2

Veja *Insights* no Gerenciador de sistemas do ONTAP para identificar as práticas recomendadas e modificações de configuração que você pode implementar em seu sistema ASA R2 para otimizar a segurança e o desempenho do cluster.

Por exemplo, suponha que você tenha servidores NTP (Network Time Protocol) configurados para o cluster. No entanto, você não sabe que você tem menos do que o número recomendado de servidores NTP necessários para o gerenciamento ideal do tempo de cluster. Para ajudá-lo a evitar problemas que podem ocorrer quando a hora do cluster é imprecisa, o Insights irá notificá-lo de que você tem poucos servidores NTP configurados e lhe dará opções para saber mais sobre esse problema, corrigi-lo ou descartá-lo.



Passos

1. No System Manager, selecione **Insights**.
2. Reveja as recomendações.

O que vem a seguir

Execute todas as ações necessárias para implementar as práticas recomendadas e otimizar a segurança e o desempenho do cluster.

Exibir eventos e trabalhos de cluster em sistemas de storage ASA R2

Use o Gerenciador de sistema do ONTAP para exibir uma lista de erros ou alertas que ocorreram em seu sistema, juntamente com as ações corretivas recomendadas. Também pode visualizar registos de auditoria do sistema e uma lista de trabalhos ativos, concluídos ou com falha.

Passos

1. No System Manager, selecione **Eventos e trabalhos**.

2. Exibir eventos e trabalhos do cluster.

Para ver isto…	Faça isso…
Eventos de cluster	Selecione **Eventos**; em seguida, selecione **log de eventos**.
Sugestões de Active IQ	Selecione **Eventos**; em seguida, selecione **sugestões Active IQ**.
Alertas do sistema	a. Selecione **alertas do sistema**. b. Selecione o alerta do sistema para o qual pretende agir. c. Confirme ou suprime o alerta.
Trabalhos de cluster	Selecione **trabalhos**.
Logs de auditoria	Selecione **Registo de auditoria**.

Envie notificações por e-mail para eventos de cluster e logs de auditoria

Configure o sistema para enviar uma notificação para endereços de e-mail específicos quando houver um evento de cluster ou entrada de log de auditoria.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Gerenciamento de notificações**, selecione .
3. Para configurar um destino de evento, selecione **Ver destinos de eventos**; em seguida, selecione **destinos de eventos**. Para configurar um destino de log de auditoria, selecione **Exibir destinos de auditoria**; em seguida, selecione **destinos de log de auditoria**.
4. + Add Selecione .
5. Introduza as informações de destino e, em seguida, selecione **Add**.

Resultado

O endereço de e-mail que você adicionou receberá agora as notificações de e-mail especificadas para eventos de cluster e logs de auditoria.

Gerenciar nós

Adicione nós do ASA R2 a um cluster do ONTAP

A partir do ONTAP 9.16.1, os sistemas de armazenamento ASA r2 suportam até 12 nós por cluster. Depois que os novos nós de um par HA forem cabeados e ligados, você precisará conectá-los ao cluster.

Antes de começar

Reúna as seguintes informações:

- O endereço IP do nó

- O endereço IP da interface de rede entre clusters
- A máscara de sub-rede entre clusters
- O gateway de rede entre clusters
- Se você quiser configurar o gerenciador de chaves integrado (OKM), você precisará da senha OKM.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione ⋮ ao lado do nó que deseja ingressar no cluster; em seguida, selecione **Adicionar nó**
3. Introduza o endereço IP de cada nó.
4. Introduza o endereço IP da interface de rede entre clusters, a máscara de sub-rede e o gateway.
5. Se você quiser configurar o gerenciador de chaves integrado (OKM), insira a senha OKM.

   Configurar o gerenciador de chaves integrado para criptografia é selecionado por padrão.

6. Selecione **Adicionar**.

Resultado

O novo par de HA é Unido ao cluster.

O que se segue?

Depois de adicionar o novo par de HA ao cluster, você pode "Habilite o acesso a dados de seus hosts SAN"nos novos nós.

Reinicie um nó em um sistema de storage ASA R2

Talvez seja necessário reinicializar um nó para manutenção, solução de problemas, atualizações de software ou outros motivos administrativos. Quando um nó é reinicializado, o parceiro de HA executa automaticamente um takeover. Em seguida, o nó do parceiro executa um giveback automático após o nó reinicializado voltar online.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione ⋮ ao lado do nó que deseja reinicializar; em seguida, selecione **Reboot**.
3. Digite o motivo pelo qual você está reiniciando o nó; em seguida, selecione **Reboot**.

   O motivo que introduzir para a reinicialização é registado no registo de auditoria do sistema.

O que se segue?

Enquanto o nó está sendo reinicializado, seu parceiro de HA realiza um takeover para que não haja interrupção no serviço de dados. Quando a reinicialização estiver concluída, o parceiro de HA executa um giveback.

Renomeie um nó em um sistema de storage ASA R2

Você pode usar o Gerenciador de sistema do ONTAP para renomear um nó no sistema ASA R2. Talvez seja necessário renomear um nó para alinhar com as convenções de nomenclatura da sua organização ou por outros motivos administrativos.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione ⋮ ao lado do nó que deseja renomear; em seguida, selecione **Renomear**.
3. Insira o novo nome para o nó e selecione **Renomear**.

Resultado

O novo nome é aplicado ao nó.

Gerenciar contas de usuários e funções em sistemas de storage ASA R2

Use o System Manager para configurar o acesso do controlador de domínio do diretório ativo, a autenticação LDAP e SAML para suas contas de usuário. Crie funções de conta de usuário para definir funções específicas que os usuários atribuídos às funções podem executar no cluster.

Configurar o acesso do controlador de domínio do diretório ativo

Configure o acesso do controlador de domínio do ative Directory (AD) ao cluster ou à VM de armazenamento para que você possa habilitar o acesso à conta do AD.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, em **ative Directory**, selecione **Configurar**.

O que se segue?

Agora você pode ativar o acesso à conta AD no seu sistema ASA R2.

Configurar o LDAP

Configure um servidor LDAP (Lightweight Directory Access Protocol) para manter centralmente as informações do usuário para autenticação.

Antes de começar

Você deve ter gerado uma solicitação de assinatura de certificado e adicionado um certificado digital de servidor assinado pela CA.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **LDAP**, ⚙ selecione .
3. Introduza o servidor LDAP necessário e as informações de encadernação; em seguida, selecione **Guardar**.

O que se segue?

Agora você pode usar o LDAP para informações e autenticação do usuário.

Configurar a autenticação SAML

A autenticação SAML (Security Assertion Markup Language) permite que os usuários sejam autenticados por um provedor de identidade seguro (IDP) em vez dos provedores de serviços diretos, como ative Directory e LDAP.

Antes de começar

- O IDP que pretende utilizar para autenticação remota tem de ser configurado.

  Consulte a documentação do IDP para obter a configuração.

- Você deve ter o URI do IDP.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **autenticação SAML**, selecione .
3. Selecione **Ativar autenticação SAML**.
4. Insira o URL do IDP e o endereço IP do sistema host; em seguida, selecione **Salvar**.

   Uma janela de confirmação exibe as informações de metadados, que foram copiadas automaticamente para a área de transferência.

5. Vá para o sistema IDP que você especificou; em seguida, copie os metadados da área de transferência para atualizar os metadados do sistema.
6. Retorne à janela de confirmação no System Manager; em seguida, selecione **Eu configurei o IDP com o URI do host ou metadados**.
7. Selecione **Logout** para ativar a autenticação baseada em SAML.

   O sistema IDP exibirá uma tela de autenticação.

O que se segue?

Agora você pode usar a autenticação SAML para suas contas de usuário.

Criar funções de conta de usuário

As funções para administradores de cluster e administradores de VM de storage são criadas automaticamente quando o cluster é inicializado. Crie funções de conta de usuário adicionais para definir funções específicas que os usuários atribuídos às funções podem executar no cluster.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **usuários e funções**, selecione .
3. Em **funções**, + Add selecione .
4. Selecione os atributos da função.

   Para adicionar vários atributos, + Add selecione .

5. Selecione **Guardar**.

Resultado

Uma nova conta de usuário é criada e está disponível para uso no sistema ASA R2.

Crie uma conta de administrador

Crie uma conta de usuário administrador para permitir que o usuário da conta execute ações específicas no cluster com base na função atribuída à conta. Para melhorar a segurança da conta, configure a autenticação multifator (MFA) quando você criar a conta.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **usuários e funções**, → selecione .
3. Em **Users**, + Add selecione .
4. Introduza um nome de utilizador e, em seguida, selecione uma função a atribuir ao utilizador.
5. Selecione o método de login do usuário e o método de autenticação.
6. Para ativar o MFA, + Add selecione ; em seguida, selecione um método de login secundário e um método de autenticação
7. Introduza uma palavra-passe para o utilizador.
8. Selecione **Guardar**.

Resultado

Uma nova conta de administrador é criada e está disponível para uso no cluster do ASA R2.

Gerenciar certificados de segurança em sistemas de storage ASA R2

Use certificados de segurança digitais para verificar a identidade de servidores remotos.

O OCSP (Online Certificate Status Protocol) valida o status de solicitações de certificados digitais de serviços ONTAP usando conexões SSL e TLS (Transport Layer Security).

Gerar uma solicitação de assinatura de certificado

Gerar uma solicitação de assinatura de certificado (CSR) para criar uma chave privada que pode ser usada para gerar um certificado público.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, → selecione ; em seguida, selecione + Generate CSR.
3. Introduza o nome comum do assunto e, em seguida, selecione o país.
4. Se pretender alterar as predefinições do GSR, selecione a utilização de chave alargada ou adicione nomes alternativos de assunto, ↙↗ More options selecione ; em seguida, efetue as atualizações pretendidas.
5. Selecione **Generate**.

Resultado

Você gerou um CSR para o qual pode ser usado para gerar um certificado público.

Adicione uma autoridade de certificação confiável

O ONTAP fornece um conjunto padrão de certificados raiz confiáveis para aplicativos que usam a Segurança da camada de Transporte (TLS). Você pode adicionar autoridades de certificação confiáveis adicionais, conforme necessário.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, →selecione .
3. Selecione **autoridades de certificação fidedignas**.
4. Introduza ou importe os detalhes do certificado; em seguida, + Add selecione .

Resultado

Você adicionou uma nova autoridade de certificação confiável ao seu sistema ASA R2.

Renove ou exclua uma autoridade de certificação confiável

As autoridades de certificação confiáveis devem ser renovadas anualmente. Se você não quiser renovar um certificado expirado, você deve excluí-lo.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, →selecione .
3. Selecione **autoridades de certificação fidedignas**.
4. Selecione a autoridade de certificação de confiança que pretende renovar ou eliminar.
5. Renovar ou eliminar a autoridade de certificação.

Para renovar a autoridade de certificação, faça isso…	Para excluir a autoridade de certificação, faça isso…
a. ⋮Selecione ; em seguida, selecione **Renew**. b. Introduza ou importe as informações do certificado; em seguida, selecione **Renew**.	a. ⋮Selecione ; em seguida, selecione **Delete**. b. Confirme que deseja excluir; em seguida, selecione **Excluir**.

Resultado

Renovou ou ou eliminou uma autoridade de certificação fidedigna existente no seu sistema ASA R2.

Adicione um certificado de cliente/servidor ou autoridades de certificação locais

Adicione um certificado de cliente/servidor ou autoridades de certificação locais para ativar serviços Web seguros.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, →selecione .
3. Selecione **certificados de cliente/servidor** ou **autoridades de certificação locais**.

4. Adicione as informações do certificado e + Add selecione .

Resultado

Adicionou um novo certificado de cliente/servidor ou autoridades locais ao seu sistema ASA R2.

Renovar ou eliminar um certificado de cliente/servidor ou autoridades de certificação locais

Os certificados de cliente/servidor e as autoridades de certificação locais devem ser renovados anualmente. Se você não quiser renovar um certificado expirado ou autoridades de certificado locais, você deve excluí-los.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de certificados, → selecione .
3. Selecione **certificados de cliente/servidor** ou **autoridades de certificação locais**.
4. Selecione o certificado que pretende renovar ou eliminar.
5. Renovar ou eliminar a autoridade de certificação.

Para renovar a autoridade de certificação, faça isso…	Para excluir a autoridade de certificação, faça isso…
a. ⋮ Selecione ; em seguida, selecione **Renew**. b. Introduza ou importe as informações do certificado; em seguida, selecione **Renew**.	⋮ Selecione ; em seguida, selecione **Delete**.

Resultado

Renovou ou ou eliminou um certificado cliente/servidor existente ou uma autoridade de certificação local no seu sistema ASA R2.

Verifique a conectividade de host no sistema de storage ASA R2

Se houver um problema com as operações de dados do host, use o Gerenciador de sistema do ONTAP para verificar se a conexão do host ao sistema de storage do ASA R2 está ativa.

Passos

1. No System Manager, selecione **Host**.

   O status de conetividade do host é indicado ao lado do nome do grupo de hosts da seguinte forma:

   - **OK**: Indica que todos os iniciadores estão conetados a ambos os nós.
   - **Parcialmente conetado**: Indica que alguns dos iniciadores não estão conetados ambos os nós.
   - **Nenhum conetado**: Indica que nenhum iniciador está conetado.

O que se segue?

Faça atualizações no seu host para corrigir problemas de conetividade. O ONTAP irá verificar novamente o

estado da ligação a cada quinze minutos.

Mantenha seu sistema de storage ASA R2

Aceda a "Documentação de manutenção do ASA R2" para saber como executar procedimentos de manutenção nos componentes do sistema ASA R2.

Saiba mais

ASA R2 para usuários avançados do ONTAP

Compare os sistemas ASA R2 com outros sistemas ONTAP

Os sistemas ASA r2 oferecem uma solução de hardware e software para ambientes exclusivamente SAN, construída com base em soluções all-flash. Os sistemas ASA r2 diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua personalidade ONTAP , camada de armazenamento e protocolos suportados.

Os seguintes sistemas são classificados como sistemas ASA r2:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Diferenças de personalidade

Em um sistema ASA R2, o software ONTAP é otimizado para oferecer suporte à funcionalidade essencial da SAN, ao mesmo tempo em que limita a visibilidade e a disponibilidade de recursos e funções que não sejam relacionados à SAN. Por exemplo, o Gerenciador de sistema em execução em um sistema ASA R2 não exibe opções para criar diretórios base para clientes nas. Esta versão simplificada do ONTAP é identificada como a personalidade *ASA R2*. O ONTAP executado em sistemas ASA é identificado como *ASA ONTAP Personality*. ONTAP executado em sistemas AFF e FAS ONTAP é identificado como a personalidade ONTAP unificada_. As diferenças entre as personalidades do ONTAP são referenciadas na referência de comando do ONTAP (páginas man), na especificação REST API e nas mensagens EMS, quando aplicável.

Você pode verificar a personalidade do seu storage da ONTAP no Gerenciador do sistema ou na CLI do ONTAP.

- No menu System Manager, selecione **Cluster > Overview**.
- Na CLI, digite: `system node show -personality -is-disaggregated`

Para sistemas ASA r2, a *personalidade* é *ASA r2* e o status de *é-desagregado* é *verdadeiro*.

A personalidade do seu sistema de storage ONTAP não pode ser alterada.

Diferenças na camada de armazenamento

Os sistemas ASA r2 usam uma camada de armazenamento simplificada que é diferente da camada de armazenamento usada pelos sistemas FAS, AFF e ASA .

Sistemas FAS, AFF e ASA

A camada de armazenamento para sistemas FAS, AFF e ASA utiliza agregados como unidade base de armazenamento. Um agregado possui um conjunto específico de discos disponíveis em um sistema de armazenamento. O agregado aloca espaço nos discos que possui para volumes para LUNs e namespaces. Com esses sistemas, os usuários do ONTAP podem criar e modificar agregados, volumes, LUNs e namespaces.

Sistemas ASA r2

Em vez de agregados, a camada de armazenamento em sistemas ASA r2 utiliza zonas de disponibilidade de armazenamento. Uma zona de disponibilidade de armazenamento é um conjunto comum de armazenamento disponível para ambos os nós de um único par de alta disponibilidade. Ambos os nós no par de alta disponibilidade têm acesso a todos os discos disponíveis em sua zona de disponibilidade de armazenamento compartilhada. Por exemplo, em um cluster ONTAP de um sistema ASA r2 de 2 nós, há uma zona de disponibilidade de armazenamento, acessível por ambos os nós do cluster. Em um cluster ONTAP de um sistema ASA r2 de 4 nós, há duas zonas de disponibilidade de armazenamento. Cada par de alta disponibilidade no cluster tem acesso a uma das zonas de disponibilidade de armazenamento.

Quando uma unidade de armazenamento (baseada em um LUN ou em um namespace NVMe) é criada, o ONTAP cria automaticamente um volume na zona de disponibilidade de armazenamento apropriada para abrigar a unidade de armazenamento. O volume recém-criado é automaticamente colocado na zona de disponibilidade de armazenamento para desempenho ideal e utilização equilibrada da capacidade. A utilização da capacidade é equilibrada dentro da zona de disponibilidade de armazenamento com base na sua versão do ONTAP. "Aprenda sobre balanceamento de capacidade em um cluster ASA r2".

Resumo das diferenças do sistema ASA r2

Os sistemas ASA r2 diferem dos sistemas FAS, AFF e ASA nas seguintes maneiras:

	ASA r2	ASA	AFF	FAS
Personalidade ONTAP	ASA r2	ASA	Unificado	Unificado
Suporte ao protocolo SAN	Sim	Sim	Sim	Sim
Suporte ao protocolo nas	Não	Não	Sim	Sim
Suporte de camada de armazenamento	Zona de disponibilidade de armazenamento	Agregados	Agregados	Agregados

Devido a essa abordagem automatizada e simplificada para o gerenciamento de armazenamento, certas opções do Gerenciador de Sistemas, comandos ONTAP e endpoints da API REST não estão disponíveis ou

têm uso limitado em um sistema ASA r2. Por exemplo, como a criação e o gerenciamento de volumes são automatizados para sistemas ASA r2, o menu **Volumes** não aparece no Gerenciador de Sistemas e o `volume create` O comando não é suportado. "Saiba mais sobre comandos ASA r2 não suportados" .

As principais diferenças entre os sistemas ASA R2 e os sistemas FAS, AFF e ASA relevantes para a interface de linha de comando (CLI) do ONTAP e API REST são descritas abaixo.

Criação de VM de armazenamento padrão com serviços de protocolo

Os novos clusters contêm automaticamente uma máquina virtual (VM) de armazenamento de dados padrão com os protocolos SAN ativados. Os LIFs de dados IP suportam os protocolos iSCSI e NVMe/TCP e utilizam o `default-data-blocks` Política de serviço por padrão.

Criação automática de volume

A criação de uma unidade de armazenamento (LUN ou namespace) cria automaticamente um volume a partir da zona de disponibilidade de armazenamento. Isso resulta em um namespace simplificado e comum. Eliminar uma unidade de armazenamento elimina automaticamente o volume associado.

Alterações no provisionamento fino e espesso

As unidades de storage são sempre provisionadas de forma fina nos sistemas de storage ASA R2. O provisionamento espesso não é suportado.

Alterações na compressão de dados

A eficiência de storage sensível à temperatura não é aplicada em sistemas ASA R2. Em sistemas ASA R2, a compactação não é baseada em dados *hot* (acessados com frequência) ou dados *cold* (acessados com pouca frequência). A compactação começa sem esperar que os dados fiquem frios.

Para mais informações

- Saiba mais "Sistemas de hardware ONTAP"sobre o .
- Consulte o suporte completo à configuração e as limitações dos sistemas ASA e ASA R2 no "NetApp Hardware Universe".
- Saiba mais sobre o "NetApp ASA".

Suporte e limitações do software ONTAP para sistemas de storage ASA R2

Embora os sistemas ASA R2 ofereçam uma ampla gama de suporte para soluções SAN, certos recursos de software ONTAP não são suportados.

Os sistemas ASA R2 não suportam o seguinte:

- Failover automático de iSCSI LIF predefinido

  Nos sistemas ASA R2, o LIF de rede padrão é compartilhado entre hosts NVMe e SCSI, portanto, não é compatível com failover automático. Para ativar o failover automático de LIF iSCSI, é "Crie um LIF apenas iSCSI"necessário . O failover automático é ativado no iSCSI Only LIFS por padrão.

  Quando o failover automático de LIF iSCSI é ativado, se ocorrer um failover de armazenamento, o iSCSI LIF é migrado automaticamente de seu nó ou porta inicial para seu nó ou porta parceiro de HA e, em seguida, volta assim que o failover for concluído. Ou, se a porta de um iSCSI LIF não for saudável, o LIF é migrado automaticamente para uma porta saudável em seu nó inicial atual e, em seguida, de volta para sua porta original quando a porta estiver funcionando novamente.

- FabricPool

- Provisionamento de espessura de LUN
- MetroCluster
- Protocolos de objetos
- ONTAP S3 SnapMirror e S3 APIs

Os sistemas ASA R2 suportam o seguinte:

- SnapLock

  "Saiba como bloquear instantâneos" No seu sistema ASA R2.

- Criptografia de camada dupla

  "Saiba como aplicar criptografia de camada dupla" Para dados no seu sistema ASA R2.

Suporte para replicação SnapMirror

A replicação SnapMirror é suportada em sistemas ASA r2 com as seguintes limitações:

- A replicação síncrona do SnapMirror não é suportada.
- O SnapMirror ActiveSync é compatível apenas entre dois sistemas ASA R2.

  Saiba mais sobre"Sincronização ativa do SnapMirror em sistemas ASA r2" .

- A replicação assíncrona do SnapMirror é suportada apenas entre dois sistemas ASA r2. A replicação assíncrona do SnapMirror não é suportada entre um sistema ASA r2 e um sistema ASA, AFF ou FAS , ou a nuvem.

  Saiba mais sobre"Políticas de replicação SnapMirror suportadas em sistemas ASA r2" .

Para mais informações

- Consulte o "NetApp Hardware Universe" para obter mais informações sobre o suporte e limitações de hardware do ASA R2.

Compatibilidade com CLI ONTAP para sistemas de storage ASA R2

Em vez de agregados, a camada de armazenamento em sistemas ASA r2 utiliza zonas de disponibilidade de armazenamento. Uma zona de disponibilidade de armazenamento é um conjunto comum de armazenamento disponível para um único par de HA. Ambos os nós no par de HA têm acesso a todos os discos disponíveis em sua zona de disponibilidade de armazenamento compartilhada. Quando uma unidade de armazenamento (LUN ou namespace NVMe) é criada, o ONTAP cria automaticamente um volume na zona de disponibilidade de armazenamento apropriada para hospedar a unidade de armazenamento.

Devido a esta abordagem simplificada à gestão do armazenamento, `storage aggregate` Os comandos não são suportados em sistemas ASA r2. Suporte para certos `lun` , `storage` e `volume` comandos e parâmetros também são limitados.

Os seguintes comandos e conjuntos de comandos não são suportados no ASA no R2:

Comandos <code> lun</code> não suportados

- `lun copy`
- `lun geometry`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

> O `lun move-in-volume` o comando é substituído pelo `lun rename` e o `vserver nvme namespace rename` comandos.

- `lun transition`

Comandos <code>storage</code> não suportados

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

Conjuntos de comandos <code>volume</code> não suportados

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Comandos e parâmetros <code>volume</code> não suportados

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  O `volume modify` o comando não está disponível quando usado em conjunto com os seguintes parâmetros:

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`

- `volume mount`
- `volume move`
- `volume offline`
- `volume rehost`
- `volume rename`
- `volume restrict`
- `volume transition-prepare-to-downgrade`
- `volume unmount`

Comandos <code> volume clone</code> não suportados

- `volume clone create`
- `volume clone split`

Comandos <code> volume SnapLock </code> não suportados

- `volume snaplock modify`

Comandos <code> volume snapshot</code> não suportados

- `volume snapshot`
- `volume snapshot autodelete modify`
- `volume snapshot policy modify`

Para mais informações

Consulte a "Referência do comando ONTAP" para obter uma lista completa dos comandos suportados

Configure um cluster do ONTAP ASA R2 usando a CLI

Recomenda-se que você "Use o Gerenciador do sistema para configurar o cluster do ONTAP ASA R2". O System Manager oferece um fluxo de trabalho guiado rápido e fácil para colocar o cluster em funcionamento. No entanto, se você estiver acostumado a trabalhar com comandos ONTAP, a interface de linha de comando (CLI) do ONTAP pode ser usada opcionalmente para a configuração do cluster. A configuração do cluster usando a CLI não oferece opções ou vantagens adicionais do que a configuração do cluster usando o System Manager.

Durante a configuração do cluster, sua máquina virtual de armazenamento de dados (VM) padrão é criada, uma unidade de armazenamento inicial é criada e suas LIFs de dados são descobertas automaticamente. Opcionalmente, você pode habilitar o sistema de nomes de domínio (DNS) para resolver nomes de host, definir seu cluster para usar o Network Time Protocol (NTS) para sincronização de tempo e ativar a criptografia de dados em repouso.

Antes de começar

Reúna as seguintes informações:

- Endereço IP de gerenciamento de cluster

  O endereço IP de gerenciamento de cluster é um endereço IPv4 exclusivo para a interface de gerenciamento de cluster usada pelo administrador do cluster para acessar a VM de armazenamento de administrador e gerenciar o cluster. Você pode obter esse endereço IP do administrador responsável pela atribuição de endereços IP na sua organização.

- Máscara de sub-rede da rede

  Durante a configuração do cluster, a ONTAP recomenda um conjunto de interfaces de rede apropriadas para sua configuração. Você pode ajustar a recomendação, se necessário.

- Endereço IP do gateway de rede
- Endereço IP do nó do parceiro
- Nomes de domínio DNS
- Endereços IP do servidor de nomes DNS
- Endereços IP do servidor NTP
- Máscara de sub-rede de dados

Passos

1. Ligue os dois nós do par de HA.
2. Mostrar os nós descobertos na rede local:

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Inicie o assistente de configuração do cluster:

   ```
   cluster setup
   ```

4. Confirme a declaração AutoSupport.
5. Introduza valores para a porta de interface de gestão de nó, endereço IP, máscara de rede e gateway predefinido.
6. Pressione **Enter** para continuar a configuração usando a interface da linha de comando; em seguida, digite **Create** para criar um novo cluster.
7. Aceite as predefinições do sistema ou introduza os seus próprios valores.
8. Depois que a configuração do primeiro nó estiver concluída, faça login no cluster.
9. Verifique se o cluster está ativo e se o primeiro nó está em funcionamento:

   ```
   system node show-discovered
   ```

10. Adicione o segundo nó ao cluster:

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. Opcionalmente, sincronize a hora do sistema no cluster

Sincronizar sem autenticação simétrica	`cluster time-service ntp server create -server <server_name>`
Sincronizar com autenticação simétrica	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. Verifique se o cluster está associado a um servidor NTP:

```
Cluster time-service ntp show
```

12. Opcionalmente, baixe e execute "ActiveIQ Config Advisor" para confirmar sua configuração.

O que se segue?

Você está pronto "configure o acesso aos dados"para de seus clientes SAN para seu sistema.

Compatibilidade com API REST para ASA R2

A API REST do ASA R2 é baseada na API REST fornecida com a personalidade ONTAP unificada, com várias alterações adaptadas às caraterísticas e capacidades únicas da personalidade do ASA R2.

Tipos de alterações de API

Há vários tipos de diferenças entre a API REST do sistema ASA R2 e a API REST ONTAP unificada disponível nos sistemas FAS, AFF e ASA. Entender os tipos de alterações ajudará você a utilizar melhor a documentação de referência de API on-line.

Novos endpoints do ASA R2 não suportados no Unified ONTAP

Vários endpoints foram adicionados à API REST do ASA R2 que não estão disponíveis com o Unified ONTAP.

Por exemplo, um novo ponto de extremidade de volume de bloco foi adicionado à API REST para sistemas ASA R2. O endpoint de volume de bloco fornece acesso a objetos de namespace LUN e NVMe, permitindo uma visualização agregada dos recursos. Isso só está disponível por meio da API REST.

Como outro exemplo, os pontos de extremidade **Storage-Units** fornecem uma visualização agregada dos LUNs e namespaces NVMe. Existem vários endpoints e todos eles são baseados ou derivados `/api/storage/storage-units` do . Você também deve rever `/api/storage/luns` e

`/api/storage/namespaces`.

Restrições sobre os métodos HTTP usados para alguns endpoints

Vários endpoints disponíveis com o ASA R2 têm restrições sobre as quais os métodos HTTP podem ser usados em comparação com o Unified ONTAP. Por exemplo, POST e DELETE não são permitidos ao usar o endpoint `/api/protocols/nvme/services` com sistemas ASA R2.

Alterações de propriedade para um endpoint e método HTTP

Algumas combinações de terminais e métodos do sistema ASA R2 não suportam todas as propriedades definidas disponíveis na personalidade unificada do ONTAP. Por exemplo, ao USAR PATCH com o endpoint `/api/storage/volumes/{uuid}`, várias propriedades não são suportadas com o ASA R2, incluindo:

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Alterações ao processamento interno

Há várias alterações na forma como o ASA R2 processa determinadas solicitações de API REST. Por exemplo, uma SOLICITAÇÃO DE EXCLUSÃO com o endpoint `/api/storage/luns/{uuid}` é processada de forma assíncrona.

Segurança aprimorada com o OAuth 2,0

OAuth 2,0 é o quadro de autorização padrão da indústria. Ele é usado para restringir e controlar o acesso a recursos protegidos com base em tokens de acesso assinados. Você pode configurar o OAuth 2,0 usando o Gerenciador de sistema para proteger os recursos do sistema ASA R2.

Depois que o OAuth 2,0 é configurado com o System Manager, o acesso pelos clientes REST API pode ser controlado. Você precisa primeiro obter um token de acesso de um servidor de autorização. Em seguida, o cliente REST passa o token para o cluster ASA R2 como um token portador usando o cabeçalho de solicitação de autorização HTTP. Consulte "Autenticação e autorização usando OAuth 2,0" para obter mais informações.

Acesse a documentação de referência da API do ASA R2 por meio da interface do usuário do Swagger

Você pode acessar a documentação de referência da API REST por meio da IU do Swagger no sistema ASA R2.

Sobre esta tarefa

Você deve acessar a página de documentação de referência do ASA R2 para obter detalhes sobre a API REST. Como parte disso, você pode procurar a string **Specifics da plataforma** para encontrar detalhes sobre o suporte do sistema ASA R2 para as chamadas e propriedades da API.

Antes de começar

Você deve ter o seguinte:

- Endereço IP ou nome de host do LIF de gerenciamento de cluster do sistema ASA R2
- Nome de usuário e senha de uma conta com autoridade para acessar a API REST

Passos

1. Digite o URL no seu navegador e pressione **Enter**

`https://<ip_address>/docs/api`

2. Inicie sessão utilizando a sua conta de administrador.

   A página de documentação da API do ASA R2 é exibida com as chamadas de API organizadas nas principais categorias de recursos.

3. Para ver um exemplo de uma chamada de API especificamente aplicável apenas aos sistemas ASA R2, role para baixo até a categoria **SAN** e clique em **OBTER /storage/storage-units**.

Recursos comuns do ONTAP suportados em sistemas ASA r2

Como os sistemas ASA r2 executam uma versão simplificada do ONTAP, muitas tarefas comuns do ONTAP e funções do System Manager são executadas da mesma forma nos sistemas ASA r2 e em outros sistemas ONTAP .

Para obter mais informações sobre recursos e funções comuns, consulte a seguinte documentação do ONTAP .

Proteção de dados

Saiba mais sobre os recursos comuns de proteção de dados compatíveis com os sistemas ASA r2.

Servidores de chave externa agrupados

Você pode configurar a conectividade com servidores de gerenciamento de chaves externas em cluster em uma máquina virtual de armazenamento. Com servidores de chaves em cluster, você pode designar servidores de chaves primários e secundários em uma máquina virtual de armazenamento. Ao registrar chaves, o ONTAP primeiro tentará acessar um servidor de chaves primário antes de tentar acessar sequencialmente os servidores secundários até que a operação seja concluída com sucesso, evitando a duplicação de chaves.

"Aprenda a configurar servidores de chaves externas em cluster.".

Gerenciamento de chaves externas para criptografia em repouso

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados.

- "Habilitar gerenciamento de chaves externas".
- "Habilitar gerenciamento de chaves externas (NVE)" .

Segurança dos dados

Saiba mais sobre os recursos comuns de segurança de dados compatíveis com os sistemas ASA r2.

Gerenciamento de acesso de administrador

A função atribuída a um administrador determina quais tarefas ele pode executar. O Gerenciador de Sistemas fornece funções predefinidas para administradores de cluster e administradores de máquinas virtuais de armazenamento. Você atribui a função ao criar a conta de administrador, ou pode atribuir uma função

diferente posteriormente.

- "Aprenda a gerenciar o acesso de administrador com o Gerenciador de Sistemas.".

Autenticação e autorização do cliente

O ONTAP utiliza métodos padrão para proteger o acesso de clientes e administradores ao armazenamento e para proteção contra vírus. Tecnologias avançadas estão disponíveis para criptografia de dados em repouso e para armazenamento de WORM. O ONTAP autentica uma máquina cliente e um usuário, verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

"Aprenda sobre autenticação e autorização de clientes" .

Autenticação OAuth 2.0

Você pode usar a estrutura de Autorização Aberta (OAuth 2.0) para controlar o acesso aos seus clusters ONTAP . O OAuth 2.0 restringe e controla o acesso a recursos protegidos usando tokens de acesso assinados.

"Saiba mais sobre a autenticação OAuth 2.0" .

Autenticação SAML e acesso de administrador

Você pode configurar e habilitar a autenticação SAML (Security Assertion Markup Language) para serviços web. O SAML autentica usuários por meio de um provedor de identidade (IdP) externo, em vez de provedores de serviços de diretório como Active Directory e LDAP.

"Aprenda a configurar a autenticação SAML" .

Rede

Saiba mais sobre os recursos de rede comuns suportados nos sistemas ASA r2.

Conformidade com o FIPS

O ONTAP está em conformidade com o padrão FIPS 140-2 (Federal Information Processing Standards) para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas, como RC4, dentro do ONTAP.

A partir da versão 9.18.1 do ONTAP , os algoritmos criptográficos de computação pós-quântica são suportados para SSL. Esses algoritmos fornecem proteção adicional contra possíveis ataques futuros de computação quântica e estão disponíveis quando o modo SSL FIPS está desativado.

- "Aprenda a configurar o FIPS para todas as conexões SSL.".

Grupos de agregação de links (LAGs)

Um grupo de interfaces, também conhecido como Grupo de Agregação de Links (LAG, na sigla em inglês), é criado combinando duas ou mais portas físicas no mesmo nó em uma única porta lógica. A porta lógica proporciona maior resiliência, maior disponibilidade e compartilhamento de carga.

"Saiba mais sobre Grupos de Agregação de Links".

Protocolos SAN

Os sistemas ASA r2 suportam todos os protocolos SAN (iSCSI, FC, NVMe/FC, NVMe/TCP).

- "Saiba mais sobre o protocolo iSCSI".
- "Saiba mais sobre o protocolo Fibre Channel (FC)".
- "Saiba mais sobre o protocolo NVMe".
  - "Aprenda a configurar o descarregamento de cópia NVMe".

    A partir do ONTAP 9.18.1, o descarregamento de cópia NVMe é suportado. O recurso de descarregamento de cópia NVMe permite que um host NVMe transfira as operações de cópia de sua CPU para a CPU do controlador de armazenamento ONTAP . O host pode copiar dados de um namespace NVMe para outro, reservando seus recursos de CPU para cargas de trabalho de aplicativos.

  - "Saiba mais sobre alocação de espaço (desmapeamento) para NVMe.".

    A partir do ONTAP 9.16.1, a desalocação de espaço (também chamada de "hole punching" e "unmap") está habilitada por padrão para namespaces NVMe. A desalocação de espaço permite que um host desaloque blocos não utilizados de namespaces para recuperar espaço.

System Manager

Você pode pesquisar diversas ações, objetos e tópicos de informação no Gerenciador de Sistemas. Você também pode pesquisar dados da tabela para entradas específicas.

"Aprenda a pesquisar, filtrar e classificar informações no Gerenciador de Sistemas.".

Obtenha ajuda

Gerencie o AutoSupport em sistemas de storage ASA R2

O AutoSupport é um mecanismo que monitora proativamente a integridade do sistema e envia mensagens automaticamente para o suporte técnico da NetApp, sua organização de suporte interno e um parceiro de suporte.

As mensagens do AutoSupport para suporte técnico são ativadas por padrão quando você configura o cluster. Você deve definir as opções corretas e ter um host de e-mail válido para que as mensagens sejam enviadas para sua organização de suporte interna. O ONTAP começa a enviar mensagens AutoSupport 24 horas depois de ativado.

Antes de começar

Você deve ser um administrador de cluster para gerenciar o AutoSupport.

Testar a conetividade do AutoSupport

Depois de configurar o cluster, você deve testar a conetividade do AutoSupport para verificar se o suporte técnico receberá mensagens geradas pelo AutoSupport.

Passos

1. No System Manager, selecione **Cluster >Settings**.
2. Ao lado de **AutoSupport**, selecione ; em seguida, **testar conetividade**.
3. Digite um assunto para a mensagem AutoSupport; em seguida, selecione **Enviar mensagem AutoSupport de teste**.

O que se segue?

Você confirmou que o suporte técnico pode receber mensagens do AutoSupport do seu sistema ASA R2, garantindo que eles tenham os dados necessários para ajudá-lo em caso de problemas.

Adicionar destinatários AutoSupport

Adicione membros da sua organização de suporte interno à lista de endereços de e-mail que recebem mensagens do AutoSupport.

Passos

1. No System Manager, selecione **Cluster >Settings**.
2. Ao lado de **AutoSupport** selecione ; em seguida, selecione **mais opções**.
3. Ao lado de **Email**, selecione ; em seguida, selecione + Add .
4. Insira o endereço de e-mail do destinatário e, em seguida, a categoria de destinatário.

   Para parceiros, selecione **Parceiro** para a categoria de destinatários. Selecione **Geral** para membros da sua organização de suporte interno.

5. Selecione Guardar.

O que se segue?

Os endereços de e-mail que você adicionou receberão novas mensagens do AutoSupport para sua categoria

específica de destinatário.

Enviar dados AutoSupport

Se ocorrer um problema no sistema ASA R2, os dados do AutoSupport podem diminuir significativamente o tempo necessário para identificar e resolver problemas.

Passos

1. No System Manager, selecione **Cluster >Settings**.
2. Ao lado de **AutoSupport**, selecione **Generate and send** (gerar e enviar).
3. Digite um assunto para a mensagem AutoSupport; em seguida, selecione **Enviar**.

O que se segue?

Os seus dados AutoSupport são enviados para o suporte técnico.

Suprimir a geração de casos de suporte

Se você estiver executando uma atualização ou manutenção em seu sistema ASA R2, talvez queira suprimir a geração de casos de suporte do AutoSupport até que sua atualização ou manutenção esteja concluída.

Passos

1. No System Manager, selecione **Cluster >Settings**.
2. Ao lado de **AutoSupport** selecione ; em seguida, selecione **suprimir geração de casos de suporte**.
3. Especifique o número de horas para suprimir a geração de casos de suporte e, em seguida, selecione os nós para os quais você não deseja que os casos sejam gerados.
4. Selecione **Enviar**.

O que se segue?

Casos AutoSupport não serão gerados durante o tempo especificado. Se você concluir sua atualização ou manutenção antes que o tempo especificado expire, você deve retomar a geração de casos de suporte imediatamente.

Retomar a geração de casos de suporte

Se tiver suprimido a geração de casos de suporte durante uma janela de atualização ou manutenção, deverá retomar a geração de casos de suporte imediatamente após a conclusão da atualização ou manutenção.

Passos

1. No System Manager, selecione **Cluster >Settings**.
2. Ao lado de **AutoSupport** selecione ; em seguida, selecione **Retomar geração de caso de suporte**.
3. Selecione os nós para os quais você deseja retomar os casos AutoSupport gerados.
4. Selecione **Enviar**.

Resultado

Os casos do AutoSupport são gerados automaticamente para o seu sistema ASA R2, conforme necessário.

Enviar e exibir casos de suporte para sistemas de storage ASA R2

Se você tiver um problema que exija assistência, use o Gerenciador de sistemas do ONTAP para enviar um caso para o suporte técnico. Você também pode usar o Gerenciador do sistema do ONTAP para exibir casos fechados ou em andamento.

Você precisa estar "Registrado no Active IQ" para visualizar os casos de suporte do seu sistema ASA r2.

Passos

1. Para enviar um caso de suporte, no Gerenciador de sistema, selecione **Cluster >Support**; em seguida, selecione **vá para o suporte NetApp**.
2. Para visualizar um caso submetido anteriormente, no System Manager, selecione **Cluster >Support**; em seguida, selecione **View my Cases**.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

ONTAP

"Aviso para ONTAP 9.16,1"

Informações sobre direitos autorais

Informações sobre marcas comerciais