Documentação do MetroCluster

ONTAP MetroCluster

NetApp
December 23, 2024

Índice

Documentação do MetroCluster

Notas de versão do MetroCluster

Novidades no suporte à configuração do MetroCluster para recursos do ONTAP

Cada versão do software de gerenciamento de dados ONTAP 9 oferece recursos novos e aprimorados que melhoram os recursos, a capacidade de gerenciamento e o desempenho das configurações do ONTAP MetroCluster.

Para obter detalhes sobre problemas conhecidos, limitações e precauções de atualização que afetam as configurações do ONTAP MetroCluster, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Recursos suportados na configuração do MetroCluster	Descrição	Disponível a partir do início
Suporte de mobilidade de dados SVM para migração de configurações do MetroCluster	O ONTAP é compatível com a migração de um par de HA que não é MetroCluster para uma configuração MetroCluster ou de uma configuração MetroCluster para um par de HA que não é MetroCluster. Não é possível migrar um SVM entre configurações do MetroCluster. "Mobilidade de dados do SVM"	ONTAP 9.16,1
Suporte de autenticação MD5.1X para grupos de pares BGP	O ONTAP suporta autenticação MD5 em grupos de pares BGP para proteger sessões BGP. Quando o MD5 está ativado, as sessões de BGP só podem ser estabelecidas e processadas entre pares autorizados, evitando possíveis interrupções da sessão por um ator não autorizado. "Configurar LIFs de IP virtual (VIP)"	ONTAP 9.16,1
Compatibilidade com MetroCluster IP para NVMe	O protocolo de host front-end NVMe/TCP é compatível com configurações IP MetroCluster de quatro nós. "Configurações DE SAN em um ambiente MetroCluster"	ONTAP 9.15,1
Suporte a storage de objetos S3 em agregados espelhados e sem espelhamento	Você pode habilitar um servidor de storage de objetos S3 em uma SVM em um agregado espelhado ou sem espelhamento em configurações MetroCluster IP e FC. "Visão geral da configuração do S3"	ONTAP 9.14,1

Recursos suportados na configuração do MetroCluster	Descrição	Disponível a partir do início
Suporte para provisionamento de um bucket do S3 em agregados espelhados e sem espelhamento em um cluster MetroCluster	Você pode criar um bucket em um agregado espelhado ou sem espelhamento nas configurações do MetroCluster. "Crie um bucket em um agregado espelhado ou sem espelhamento em uma configuração do MetroCluster"	ONTAP 9.12,1
Compatibilidade com MetroCluster IP para NVMe	O protocolo NVMe/FC é compatível com configurações MetroCluster IP de quatro nós. "Configurações DE SAN em um ambiente MetroCluster"	ONTAP 9.12,1
Suporte a IPsec para protocolo de host front-end em configurações de conexão de malha MetroCluster IP e MetroCluster	O suporte IPsec para protocolo de host front-end (como NFS e iSCSI) está disponível nas configurações de conexão de malha do MetroCluster IP e MetroCluster. "Configurar a segurança IP (IPsec) através da criptografia por fio"	ONTAP 9.11,1
Grupos de consistência	Os grupos de consistência são compatíveis com as configurações do MetroCluster.	ONTAP 9,7
Espelhos FabricPool nas configurações do MetroCluster	Você pode configurar um FabricPool espelhado nas configurações do MetroCluster para categorizar dados inativos em duas zonas de falha diferentes. "Configurando armazenamentos de objetos para FabricPool em uma configuração MetroCluster"	ONTAP 9,7
Recuperação de desastres da SVM	As máquinas virtuais de storage ativo (SVMs) em uma configuração do MetroCluster podem ser usadas como fontes com o recurso de recuperação de desastres do SnapMirror SVM.	ONTAP 9,5

Novidades nos recursos do MetroCluster

Saiba mais sobre os novos recursos do MetroCluster.

Recursos suportados na configuração do MetroCluster	Descrição e onde saber mais	Disponível a partir do início
Atualização de firmware do Fibrebridge usando credenciais	Você pode atualizar o firmware em bridges do Fibrebridge usando credenciais se elas forem necessárias pelo servidor para baixar o pacote de firmware. "Atualize o firmware em uma ponte FibreBridge"	ONTAP 9.16,1
Suporte IP MetroCluster para criptografia de ponta a ponta	A criptografia de ponta a ponta é compatível com sistemas AFF A400, FAS8300 e FAS8700 para criptografar o tráfego de back-end, como NVlog e dados de replicação de storage, entre os locais em uma configuração IP do MetroCluster. "Configurar criptografia de ponta a ponta em uma configuração IP do MetroCluster"	ONTAP 9.15,1
Aumento do limite de volume para configurações de IP MetroCluster de quatro nós em sistemas AFF A800 e AFF C800	Nas configurações IP do MetroCluster de quatro nós, os seguintes limites de volume para sistemas AFF A800 e AFF C800 aumentaram: • O número máximo de volumes FlexVol por agregado aumentou de 200 para 625. • O número máximo de volumes FlexVol por nó aumentou de 800 para 1250. • O número máximo de volumes FlexVol por par de alta disponibilidade (HA) aumentou de 1600 para 2500.	ONTAP 9.15,1
Aumento do limite de volume para configurações de IP MetroCluster de quatro nós em sistemas AFF A900	Nas configurações IP do MetroCluster de quatro nós, os seguintes limites de volume para sistemas AFF A900 aumentaram: • O número máximo de volumes FlexVol por agregado aumentou de 200 para 625. • O número máximo de volumes FlexVol por nó aumentou de 800 para 1250. • O número máximo de volumes FlexVol por par de alta disponibilidade (HA) aumentou de 1600 para 2500.	ONTAP 9.14,1
Transição do MetroCluster FC para o MetroCluster IP usando um switch compartilhado para storage conetado MetroCluster IP e Ethernet	Você pode fazer a transição de uma configuração MetroCluster FC para uma MetroCluster IP sem interrupções usando um switch de storage compartilhado. "Transição de uma configuração IP do MetroCluster FC para uma configuração IP do MetroCluster sem interrupções (ONTAP 9.8 e posterior)"	ONTAP 9.13,1

Recursos suportados na configuração do MetroCluster	Descrição e onde saber mais	Disponível a partir do início
Transições ininterruptas de uma configuração de FC MetroCluster de oito nós para uma configuração IP MetroCluster	Você pode migrar workloads e dados de uma configuração MetroCluster FC de oito nós existente para uma nova configuração MetroCluster IP sem interrupções. "Transição de uma configuração MetroCluster FC para uma MetroCluster IP sem interrupções"	ONTAP 9.13,1
Upgrades de configuração IP MetroCluster de quatro nós usando switchover e switchback	Você pode atualizar controladores em uma configuração IP MetroCluster de quatro nós usando switchover e switchback com `system controller replace` comandos. "Atualize controladores em uma configuração IP MetroCluster de quatro nós"	ONTAP 9.13,1
O switchover não planejado automático assistido por mediador (MAUSO) é acionado para um desligamento ambiental	Se um site desligar graciosamente devido a um desligamento ambiental, MAUSO é acionado. "Como o Mediador ONTAP suporta o switchover não planejado automático"	ONTAP 9.13,1
Suporte para configurações de IP MetroCluster de oito nós	Você pode atualizar os controladores e o storage em uma configuração IP do MetroCluster de oito nós expandindo a configuração para se tornar uma configuração temporária de doze nós e removendo os grupos de DR antigos. "Atualizando uma configuração de IP MetroCluster de quatro nós"	ONTAP 9.13,1
Conversão de configuração IP do MetroCluster para uma configuração de switch MetroCluster de armazenamento compartilhado	Você pode converter uma configuração IP MetroCluster para uma configuração de switch MetroCluster de armazenamento compartilhado. "Substituição de um switch IP"	ONTAP 9.13,1
Recurso de comutação forçada automática do MetroCluster em uma configuração IP do MetroCluster	Você pode habilitar o recurso de switchover forçado automático do MetroCluster em uma configuração IP do MetroCluster. Este recurso é uma extensão do recurso de switchover não planejado assistido por Mediador (MAUSO). "Limitações de comutação automática"	ONTAP 9.12,1

Recursos suportados na configuração do MetroCluster	Descrição e onde saber mais	Disponível a partir do início
S3 em um SVM em um agregado sem espelhamento em uma configuração MetroCluster IP	Você pode habilitar um servidor de storage de objetos do ONTAP Simple Storage Service (S3) em uma SVM em um agregado sem espelhamento em uma configuração IP do MetroCluster. "Configuração do S3 com o Gerenciador de sistemas e a CLI do ONTAP"	ONTAP 9.12,1
Transição de uma configuração MetroCluster FC para uma configuração AFF A250 ou FAS500f MetroCluster IP	Você pode fazer a transição de uma configuração MetroCluster FC para uma configuração AFF A250 ou FAS500f MetroCluster IP. "Mova as conexões do cluster local"	ONTAP 9.11,1
Configuração do endereço IP MetroCluster da camada 3 nas configurações IP do MetroCluster	Você pode editar o endereço IP, a máscara de rede e o gateway do MetroCluster para nós em uma configuração da camada 3. "Modificação de endereço, máscara de rede e gateway em um IP MetroCluster"	ONTAP 9.10,1
Atualização simplificada do controlador de nós em uma configuração de MetroCluster FC	O procedimento de atualização para o processo de atualização usando switchover e switchback foi simplificado. "Atualização de controladores em uma configuração MetroCluster FC usando switchover e switchback"	ONTAP 9.10,1
Suporte IP para link compartilhado na camada 3	As configurações IP do MetroCluster podem ser implementadas com conexões back-end roteadas por IP (camada 3). "Considerações para redes de grande área da camada 3"	ONTAP 9.9,1
Suporte para clusters de 8 nós	Clusters permanentes de 8 nós são compatíveis com configurações de IP e conexão de malha. "Instalação e cabeamento de componentes MetroCluster"	ONTAP 9.9,1
Interface simplificada para gerenciar operações de IP MetroCluster com o System Manager	Você pode gerenciar as operações do IP MetroCluster com o Gerenciador do sistema, incluindo a configuração de sites do IP MetroCluster, o emparelhamento dos sites e a configuração dos clusters. "Gerenciar sites do MetroCluster"	ONTAP 9,8

Recursos suportados na configuração do MetroCluster	Descrição e onde saber mais	Disponível a partir do início
Comutação IP MetroCluster e switchback com o Gerenciador de sistemas	Você pode usar o Gerenciador de sistema para executar todas as etapas de procedimentos de comutação e switchback planejados ou não planejados para configurações de IP MetroCluster. "Switchover e switchback do MetroCluster"	ONTAP 9,8
Transição das configurações MetroCluster FC para MetroCluster IP	A transição de workloads e dados de uma configuração MetroCluster FC de quatro nós existente para uma nova configuração MetroCluster IP é compatível. "Atualize, atualize ou expanda a configuração do MetroCluster" "Transição do MetroCluster FC para o MetroCluster IP"	ONTAP 9,8
Novos procedimentos de atualização e atualização	A atualização ou atualização de hardware de configurações de FC e IP do MetroCluster de quatro nós é compatível. "Atualize, atualize ou expanda a configuração do MetroCluster" "Transição do MetroCluster FC para o MetroCluster IP"	ONTAP 9,8
Agregados não espelhados	Agregados não espelhados são compatíveis com configurações MetroCluster IP. "Considerações para agregados sem espelhamento"	ONTAP 9,8
Switches compatíveis com MetroCluster	As configurações IP do MetroCluster podem suportar switches que não são validados pela NetApp, desde que estejam em conformidade com as especificações da NetApp. "Considerações para usar switches compatíveis com MetroCluster"	ONTAP 9,7

Recursos suportados na configuração do MetroCluster	Descrição e onde saber mais	Disponível a partir do início
Compartilhamento de rede de camada privada 2	As configurações IP do MetroCluster com switches Cisco compatíveis podem compartilhar redes existentes para ISLs, em vez de usar ISLs MetroCluster dedicados. Versões anteriores do ONTAP requerem ISLs dedicados. Os switches IP do MetroCluster são dedicados à configuração do MetroCluster e não podem ser compartilhados. Apenas as portas ISL MetroCluster nos switches IP MetroCluster podem se conetar aos switches compartilhados. Se estiver usando uma rede compartilhada, o cliente será responsável por atender aos requisitos de rede MetroCluster na rede compartilhada. "Instalação e configuração IP do MetroCluster"	ONTAP 9,6
Switchover e switchback do MetroCluster	Você pode permitir que um site de cluster assuma as tarefas de outro site de cluster. Essa funcionalidade permite facilitar a manutenção ou a recuperação de desastres. "Switchover e switchback do MetroCluster"	ONTAP 9,6

O que há de novo no suporte à plataforma IP MetroCluster

Saiba o que há de novo no suporte à plataforma IP MetroCluster.

Suporte de plataforma

Plataformas compatíveis em configurações IP do MetroCluster	Disponível a partir do início
AFF A70, AFF A90, AFF A1K	ONTAP 9.15,1
ASA A150, ASA A250, ASA A400, ASA A800, ASA A900, ASA C250, ASA C400, ASA C800	ONTAP 9.14,1
AFF A150	ONTAP 9.13,1 ONTAP 9.12.1P1 ONTAP 9.11.1P8 ONTAP 9.10.1P12

Plataformas compatíveis em configurações IP do MetroCluster	Disponível a partir do início
AFF C250, AFF C400, AFF C800	ONTAP 9.12.1P1 ONTAP 9.13,1 GA
AFF A900	ONTAP 9.10,1
AFF A250	ONTAP 9,8
FAS500f	ONTAP 9,8
ASA AFF A220, ASA AFF A250, ASA AFF A400, ASA AFF A700, ASA AFF A800	ONTAP 9,7
AFF A320	ONTAP 9.6P3
AFF A220, FAS2750	ONTAP 9,6
AFF A300, FAS8200	ONTAP 9,5

Suporte do interrutor

Switches IP Broadcom	Disponível a partir do início
BES-53248	ONTAP 9,6

Switches IP Cisco	Disponível a partir do início
Nexus 9336C-FX2	ONTAP 9.9,1
9336C	ONTAP 9,8

Switches NVIDIA	Disponível a partir do início
Várias configurações de IP MC no mesmo switch NVIDIA SN2100	ONTAP 9.14,1
SN2100	ONTAP 9.12,1

Novidades no suporte à plataforma MetroCluster FC e switch

Suporte de plataforma

Plataformas compatíveis em configurações de MetroCluster FC	Disponível a partir do início
AFF A900	ONTAP 9.10,1
ASA AFF A700 e ASA AFF A400	ONTAP 9.7P5
AFF A400 e FAS8300	ONTAP 9,7
AFF A300 e FAS8200	ONTAP 9,5

Suporte do interrutor

Switches Brocade FC	Disponível a partir do início
G720	ONTAP 9,8
G620-1, G630-1	ONTAP 9,8
G630	ONTAP 9,6

O que há de novo no suporte do ONTAP Mediator

Novas melhorias para o Mediador ONTAP são fornecidas com cada versão. Eis as novidades.

Para obter detalhes sobre como instalar ou atualizar o ONTAP Mediator na configuração do MetroCluster, acesse "Prepare-se para instalar o serviço Mediador ONTAP".

Capacidade do mediador ONTAP	Versão de ONTAP
O switchover não planejado automático assistido por mediador (MAUSO) é suportado no caso de um desligamento ambiental. Se um site desligar graciosamente devido a um desligamento ambiental, MAUSO é acionado. "Como o Mediador ONTAP suporta o switchover não planejado automático"	ONTAP 9.13,1
Suporte inicial para o serviço ONTAP Mediator em configurações IP do MetroCluster	ONTAP 9,7

Novidades no suporte ao tiebreaker do MetroCluster

As melhorias no software tiebreaker MetroCluster são fornecidas em cada versão. Veja o

que há de novo em lançamentos recentes do MetroCluster Tiebreaker.

Melhorias

Versão de desempate do ONTAP	Melhorias
1.6P1	• Atualização de bibliotecas de suporte • Melhorias de segurança
1,6	• Maior facilidade de instalação • Atualização de bibliotecas de suporte • Melhorias de segurança
1,5	• Atualização de bibliotecas de suporte • Melhorias de segurança
1,4	• Atualização de bibliotecas de suporte

Matriz de suporte de SO

A tabela a seguir indica os sistemas operacionais suportados para cada versão do tiebreaker.

SO para desempate	1.6P1	1,6	1,5	1,4
Rocky Linux 9,4	Sim	Não	Não	Não
Rocky Linux 9,0	Não	Sim	Não	Não
Rocky Linux 8,10	Sim	Não	Não	Não
Chapéu vermelho 9,4	Sim	Não	Não	Não
Chapéu vermelho 9,3	Não	Não	Não	Não
Chapéu vermelho 9,2	Sim	Sim	Não	Não
Chapéu vermelho 9,1	Não	Sim	Não	Não
Chapéu vermelho 9,0	Não	Sim	Não	Não

Red Hat 8,11 - 9,0	Não	Sim	Não	Não
Chapéu vermelho 8,10	Sim	Sim	Não	Não
Chapéu vermelho 8,9	Não	Sim	Não	Não
Chapéu vermelho 8,8	Sim	Sim	Não	Não
Red Hat 8,1 - 8,7	Não	Sim	Sim	Sim
Red Hat 7 - 7,9	Não	Não	Não	Sim
CentOS 7 - 7,9	Não	Não	Não	Sim

Instale um MetroCluster conectado à malha

Visão geral

Para instalar a configuração do MetroCluster conectado à malha, você precisa executar vários procedimentos na ordem correta.

- "Prepare-se para a instalação e entenda todos os requisitos".
- "Escolha o procedimento de instalação correto"
- "Faça o cabo dos componentes"
- "Configure o software"
- "Teste a configuração"

Prepare-se para a instalação do MetroCluster

Diferenças entre as configurações do ONTAP MetroCluster

As várias configurações do MetroCluster têm diferenças importantes nos componentes necessários.

Em todas as configurações, cada um dos dois locais do MetroCluster é configurado como um cluster do ONTAP. Em uma configuração de MetroCluster de dois nós, cada nó é configurado como um cluster de nó único.

Recurso	Configurações IP	Configurações conectadas à malha		Configurações elásticas	
		Quatro ou oito nós	* Dois nós*	* Dois nós bridge-attached*	**Conexão direta de dois nós**
Número de controladores	Quatro ou oito*	Quatro ou oito	Dois	Dois	Dois
Usa uma malha de storage de switch FC	Não	Sim	Sim	Não	Não
Usa uma malha de storage de switch IP	Sim	Não	Não	Não	Não
Usa pontes FC para SAS	Não	Sim	Sim	Sim	Não
Usa o storage SAS com conexão direta	Sim (apenas anexo local)	Não	Não	Não	Sim

Suporta ADP	Sim (começando com ONTAP 9.4)	Não	Não	Não	Não
Suporta HA local	Sim	Sim	Não	Não	Não
Compatível com o switchover não planejado automático do ONTAP (AUSO)	Não	Sim	Sim	Sim	Sim
Compatível com agregados sem espelhamento	Sim (começando com ONTAP 9.8)	Sim	Sim	Sim	Sim
Compatível com LUNs de array	Não	Sim	Sim	Sim	Sim
Suporta o Mediador ONTAP	Sim (começando com ONTAP 9.7)	Não	Não	Não	Não
Compatível com o tiebreaker MetroCluster	Sim (não em combinação com o Mediador ONTAP)	Sim	Sim	Sim	Sim
Suportes Todos os arrays SAN	Sim	Sim	Sim	Sim	Sim

Importante

Observe as seguintes considerações para configurações de IP MetroCluster de oito nós:

- As configurações de oito nós são suportadas a partir do ONTAP 9.9,1.
- Somente switches MetroCluster validados pela NetApp (solicitados pela NetApp) são compatíveis.
- Configurações que usam conexões de back-end roteadas por IP (camada 3) não são suportadas.
- As configurações que usam redes de camada privada compartilhada 2 não são suportadas.
- As configurações que usam um switch compartilhado Cisco 9336C-FX2 não são suportadas.

Suporte para todos os sistemas de storage SAN nas configurações do MetroCluster

Alguns dos All SAN Arrays (ASAs) são suportados nas configurações do MetroCluster. Na documentação do MetroCluster, as informações dos modelos AFF aplicam-se ao sistema ASA correspondente. Por exemplo, todo o cabeamento e outras informações do sistema AFF A400 também se aplicam ao sistema ASA AFF A400.

As configurações de plataforma compatíveis estão listadas no "NetApp Hardware Universe".

Peering de clusters

Cada site do MetroCluster é configurado como um ponto do site do parceiro. Você deve estar familiarizado com os pré-requisitos e diretrizes para configurar as relações de peering. Isso é importante ao decidir se usar portas compartilhadas ou dedicadas para esses relacionamentos.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar que a conetividade entre os requisitos de porta, endereço IP, sub-rede, firewall e nomenclatura de cluster é atendida.

Requisitos de conetividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

  Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.

> O ONTAP 9 permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

  Você pode usar vários IPspaces para fazer pares com vários clusters. A conetividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

  As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de

interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Serviço ICMP
- TCP para os endereços IP de todos os LIFs entre clusters nas portas 10000, 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

A política de firewall entre clusters padrão permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Considerações ao usar portas dedicadas

Ao determinar se o uso de uma porta dedicada para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alteração e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o uso de uma porta dedicada é a melhor solução de rede entre clusters:

- Se a quantidade de largura de banda da WAN disponível for semelhante à das portas LAN e o intervalo de replicação for tal que a replicação ocorra enquanto a atividade do cliente regular existe, você deve dedicar portas Ethernet para replicação entre clusters para evitar a contenção entre replicação e os protocolos de dados.
- Se a utilização da rede gerada pelos protocolos de dados (CIFS, NFS e iSCSI) for tal que a utilização da rede seja superior a 50%, dedique portas para replicação para permitir desempenho não degradado se ocorrer um failover de nó.
- Quando portas físicas de 10 GbE ou mais rápidas são usadas para dados e replicação, você pode criar portas VLAN para replicação e dedicar as portas lógicas para replicação entre clusters.

  A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.

Considerações ao compartilhar portas de dados

Ao determinar se o compartilhamento de uma porta de dados para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alterações e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o compartilhamento de portas de dados é a melhor solução de conetividade entre clusters:

- Para uma rede de alta velocidade, como uma rede 40-Gigabit Ethernet (40-GbE), uma quantidade

suficiente de largura de banda local da LAN pode estar disponível para executar a replicação nas mesmas portas de 40 GbE que são usadas para acesso aos dados.

Em muitos casos, a largura de banda da WAN disponível é muito menor do que a largura de banda da LAN de 10 GbE.

- Todos os nós no cluster podem ter que replicar dados e compartilhar a largura de banda da WAN disponível, tornando o compartilhamento da porta de dados mais aceitável.
- O compartilhamento de portas para dados e replicação elimina as contagens de portas extras necessárias para dedicar portas para replicação.
- O tamanho máximo da unidade de transmissão (MTU) da rede de replicação será o mesmo tamanho que o utilizado na rede de dados.
- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.
- Quando as portas de dados para replicação entre clusters são compartilhadas, as LIFs entre clusters podem ser migradas para qualquer outra porta compatível com clusters no mesmo nó para controlar a porta de dados específica usada para replicação.

Considerações para configurações do MetroCluster com compartimentos de disco nativos ou LUNs de array

A configuração MetroCluster dá suporte a instalações com apenas compartimentos de disco nativos (NetApp), apenas LUNs de array ou uma combinação de ambos.

Os sistemas AFF não são compatíveis com LUNs de array.

Informações relacionadas

"Fazer o cabeamento de uma configuração MetroCluster conectada à malha"

"Planejamento e instalação de uma configuração MetroCluster com LUNs de array"

"Referência e requisitos de instalação da virtualização do FlexArray"

Considerações ao fazer a transição do modo 7 para o ONTAP

Você precisa ter a nova configuração do MetroCluster totalmente configurada e operacional antes de usar as ferramentas de transição para mover dados de uma configuração do MetroCluster de 7 modos para uma configuração do ONTAP. Se a configuração do modo 7 usar os switches Brocade 6510, a nova configuração poderá compartilhar as malhas existentes para reduzir os requisitos de hardware.

Se você tiver switches Brocade 6510 e planeja compartilhar as malhas de switch entre o 7-Mode Fabric MetroCluster e o MetroCluster em execução no ONTAP, use o procedimento específico para configurar os componentes do MetroCluster.

"Configuração do hardware do MetroCluster para compartilhar uma malha de FC Brocade 6510 de 7 modos durante a transição"

Considerações para ISLs

Você precisa determinar quantos ISLs você precisa para cada malha de switch FC na configuração do MetroCluster. A partir do ONTAP 9.2, em alguns casos, em vez de dedicar switches FC e ISLs a cada configuração individual do MetroCluster, você pode compartilhar os mesmos quatro switches.

Considerações sobre compartilhamento de ISL (ONTAP 9.2)

A partir do ONTAP 9.2, você pode usar o compartilhamento ISL nos seguintes casos:

- Configurações de um MetroCluster de dois nós e um de quatro nós
- Duas configurações MetroCluster de quatro nós separadas
- Duas configurações de MetroCluster de dois nós separadas
- Dois grupos de DR em uma configuração de MetroCluster de oito nós

O número de ISLs necessários entre os switches compartilhados depende da largura de banda dos modelos de plataforma conetados aos switches compartilhados.

Considere os seguintes aspetos de sua configuração ao determinar quantos ISLs você precisa.

- Dispositivos que não sejam MetroCluster não devem ser conetados a nenhum dos switches FC que fornecem a conectividade MetroCluster de back-end.
- O compartilhamento ISL é suportado em todos os switches, exceto os switches Cisco 9250i e Cisco 9148.
- Todos os nós precisam estar executando o ONTAP 9.2 ou posterior.
- O cabeamento do switch FC para compartilhamento ISL é o mesmo que para o cabeamento MetroCluster de oito nós.
- Os arquivos RCF para compartilhamento ISL são os mesmos que para o cabeamento MetroCluster de oito nós.
- Você deve verificar se todas as versões de hardware e software são suportadas.

  "NetApp Hardware Universe"

- A velocidade e o número de ISLs devem ser dimensionados para suportar a carga do cliente em ambos os sistemas MetroCluster.
- Os ISLs de back-end e os componentes de back-end devem ser dedicados apenas à configuração do MetroCluster.
- O ISL deve usar uma das velocidades suportadas: 4 Gbps, 8 Gbps, 16 Gbps ou 32 Gbps.
- Os ISLs em um tecido devem ter a mesma velocidade e comprimento.
- Os ISLs em uma malha devem ter a mesma topologia. Por exemplo, todos eles devem ser links diretos, ou se o seu sistema usa WDM, então todos eles devem usar WDM.

Considerações ISL específicas da plataforma

O número de ISLs recomendados é específico do modelo de plataforma. A tabela a seguir mostra os requisitos ISL para cada modelo de tecido por plataforma. Assume que cada ISL tem uma capacidade de 16 Gbps.

Modelo de plataforma	Número recomendado de ISLs por grupo de RD de quatro nós (por malha de switch)
AFF A900 e FAS9500	Oito
AFF A700	Seis
FAS9000	Seis
8080	Quatro
Todos os outros	Dois

Se a malha do switch oferecer suporte a oito nós (parte de uma configuração de MetroCluster de oito nós ou duas configurações de quatro nós que estão compartilhando ISLs), o número total recomendado de ISLs para a malha é a soma necessária para cada grupo de DR de quatro nós. Por exemplo:

- Se o grupo de RD 1 incluir quatro sistemas AFF A700, ele precisará de seis ISLs.
- Se o grupo de RD 2 incluir quatro sistemas FAS8200, ele precisará de dois ISLs.
- O número total de ISLs recomendados para a estrutura do switch é de oito.

Considerações sobre o uso de equipamentos TDM/WDM com configurações MetroCluster conetadas à malha

A ferramenta Hardware Universe fornece algumas notas sobre os requisitos que os equipamentos de Multiplexagem por Divisão de tempo (TDM) ou Multiplexagem por Divisão de comprimento de onda (WDM) devem atender para trabalhar com uma configuração MetroCluster conetada à malha. Essas notas também incluem informações sobre várias configurações, que podem ajudá-lo a determinar quando usar a entrega em ordem (IOD) de quadros ou entrega fora de ordem (ODE) de quadros.

Um exemplo de tais requisitos é que o equipamento TDM/WDM deve suportar o recurso de agregação de links (entroncamento) com políticas de roteamento. A ordem de entrega (IOD ou OOD) de quadros é mantida dentro de um switch e é determinada pela política de roteamento que está em vigor.

"NetApp Hardware Universe"

A tabela a seguir fornece as políticas de roteamento para configurações que contêm switches Brocade e switches Cisco:

Interrutores	Configuração das configurações do MetroCluster para IOD	Configuração das configurações do MetroCluster para ODE

Brocade	• AptPolicy deve ser definido como 1 • O DLS tem de estar definido como Off (Desligado) • IOD deve ser definido como On (ligado)	• AptPolicy deve ser definido como 3 • O DLS tem de estar definido para ON (ligado) • IOD deve ser definido como Off (Desligado)
Cisco	Políticas para o VSAN designado pela FCVI: • Política de balanceamento de carga: Srcid e dstid • IOD deve ser definido como On (ligado) Políticas para o VSAN designado para armazenamento: • Política de balanceamento de carga: Srcid, dstid e oxid • O VSAN não deve ter a opção de garantia na ordem definida	Não aplicável

Quando usar IOD

É melhor usar IOD se for suportado pelos links. As configurações a seguir suportam IOD:

- Um único ISL
- O ISL e o link (e o equipamento de link, como TDM/WDM, se usado) suportam configuração para IOD.
- Um único tronco, e os ISLs e os links (e o equipamento de link, como TDM/WDM, se usados) suportam configuração para IOD.

Quando usar OOD

- Você pode usar O ODE para todas as configurações que não oferecem suporte para IOD.
- Você pode usar ODE para configurações que não suportam o recurso de entroncamento.

Usando dispositivos de criptografia

Ao usar dispositivos de criptografia dedicados no ISL ou criptografia em dispositivos WDM na configuração do MetroCluster, você deve atender aos seguintes requisitos:

- Os dispositivos de criptografia externos ou o equipamento WDM foram auto-certificados pelo fornecedor com o switch FC em questão.

  A auto-certificação deve abranger o modo de funcionamento (como entroncamento e encriptação).

- A latência adicionada devido à criptografia não deve ser superior a 10 microssegundos.

Requisitos para usar um switch Brocade DCX 8510-8

Ao se preparar para a instalação do MetroCluster, você deve entender a arquitetura de hardware do MetroCluster e os componentes necessários.

- Os switches DCX 8510-8 usados nas configurações do MetroCluster devem ser adquiridos na NetApp.
- Para escalabilidade, você deve deixar uma parte de porta entre as configurações do MetroCluster se estiver cabendo apenas dois Metroclusters em módulos 4x48 portas. Isso permite que você expanda o uso de portas nas configurações do MetroCluster sem precisar reiniciar.
- Cada switch Brocade DCX 8510-8 na configuração MetroCluster deve ser configurado corretamente para as portas ISL e conexões de armazenamento. Para o uso da porta, consulte a seção a seguir"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior": .
- Os ISLs não podem ser compartilhados e cada MetroCluster requer dois ISLs para cada malha.
- O switch DCX 8510-8 usado para conetividade MetroCluster de back-end não deve ser usado para qualquer outra conetividade.

  Dispositivos não MetroCluster não devem ser conetados a esses switches e o tráfego não MetroCluster não deve fluir através dos switches DCX 8510-8.

- Uma placa de linha pode ser conetada a Metroclusters ONTAP **ou** ONTAP 7-Mode Metroclusters.

Os ficheiros RCF não estão disponíveis para este parâmetro.

A seguir estão os requisitos para usar dois switches Brocade DCX 8510-8:

- Você deve ter um switch DCX 8510-8 em cada local.
- Você deve usar um mínimo de dois blades de 48 portas que contêm 16GB SFPs em cada switch.

A seguir estão os requisitos para usar quatro switches DCX 8510-8 em cada local em uma configuração MetroCluster:

- Você deve ter dois switches DCX 8510-8 em cada local.
- Você deve usar pelo menos um blade de 48 portas para cada switch DCX 8510-8.
- Cada blade é configurado como um switch virtual usando malhas virtuais.

Os seguintes produtos NetApp não são suportados pelos switches Brocade DCX 8510-8:

- Config Advisor
- Monitor de integridade da malha
- MyAutoSupport (riscos do sistema podem mostrar falsos positivos)
- Active IQ Unified Manager (anteriormente Gerenciador Unificado da OnCommand)

Certifique-se de que todos os componentes necessários para esta configuração estão na "Ferramenta de Matriz de interoperabilidade do NetApp". Leia a seção de notas na ferramenta de Matriz de interoperabilidade para obter informações sobre configurações suportadas.

Considerações ao usar agregados sem espelhamento

Considerações ao usar agregados sem espelhamento

Se a sua configuração incluir agregados sem espelhamento, você precisa estar ciente de possíveis problemas de acesso que seguem as operações de switchover.

Considerações para agregados sem espelhamento ao fazer manutenção que requer desligamento de energia

Se você estiver executando um switchover negociado por motivos de manutenção que exigem desligamento de energia em todo o local, primeiro deverá ficar offline manualmente todos os agregados sem espelhamento pertencentes ao local de desastre.

Se você não colocar nenhum agregado sem espelhamento off-line, os nós no site sobrevivente podem ficar inativos devido a panics de vários discos. Isso pode ocorrer se agregados comutados por espelhamento ficarem off-line ou estiverem ausentes, devido à perda de conectividade com storage no local de desastre. Este é o resultado de um desligamento de energia ou uma perda de ISLs.

Considerações para agregados sem espelhamento e namespaces hierárquicos

Se você estiver usando namespaces hierárquicos, você deve configurar o caminho de junção para que todos os volumes nesse caminho estejam apenas em agregados espelhados ou apenas em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados no caminho de junção pode impedir o acesso aos agregados sem espelhamento após a operação de comutação.

Considerações para agregados sem espelhamento e volumes de metadados CRS e volumes raiz de dados SVM

O volume de metadados do serviço de replicação de configuração (CRS) e os volumes raiz de dados do SVM devem estar em um agregado espelhado. Não é possível mover esses volumes para um agregado sem espelhamento. Se eles estiverem em um agregado sem espelhamento, as operações de comutação negociadas e switchback serão vetadas. O comando MetroCluster check fornece um aviso se for esse o caso.

Considerações para agregados sem espelhamento e SVMs

Os SVMs devem ser configurados somente em agregados espelhados ou somente em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados pode resultar em uma operação de switchover que excede 120 segundos e resultar em uma interrupção de dados se os agregados sem espelhamento não ficarem online.

Considerações para agregados sem espelhamento e SAN

Nas versões ONTAP anteriores a 9,9.1, um LUN não deve ser localizado em um agregado sem espelhamento. Configurar um LUN em um agregado sem espelhamento pode resultar em uma operação de switchover que excede 120 segundos e uma interrupção de dados.

Uso de firewall em sites da MetroCluster

Considerações sobre o uso de firewall em sites da MetroCluster

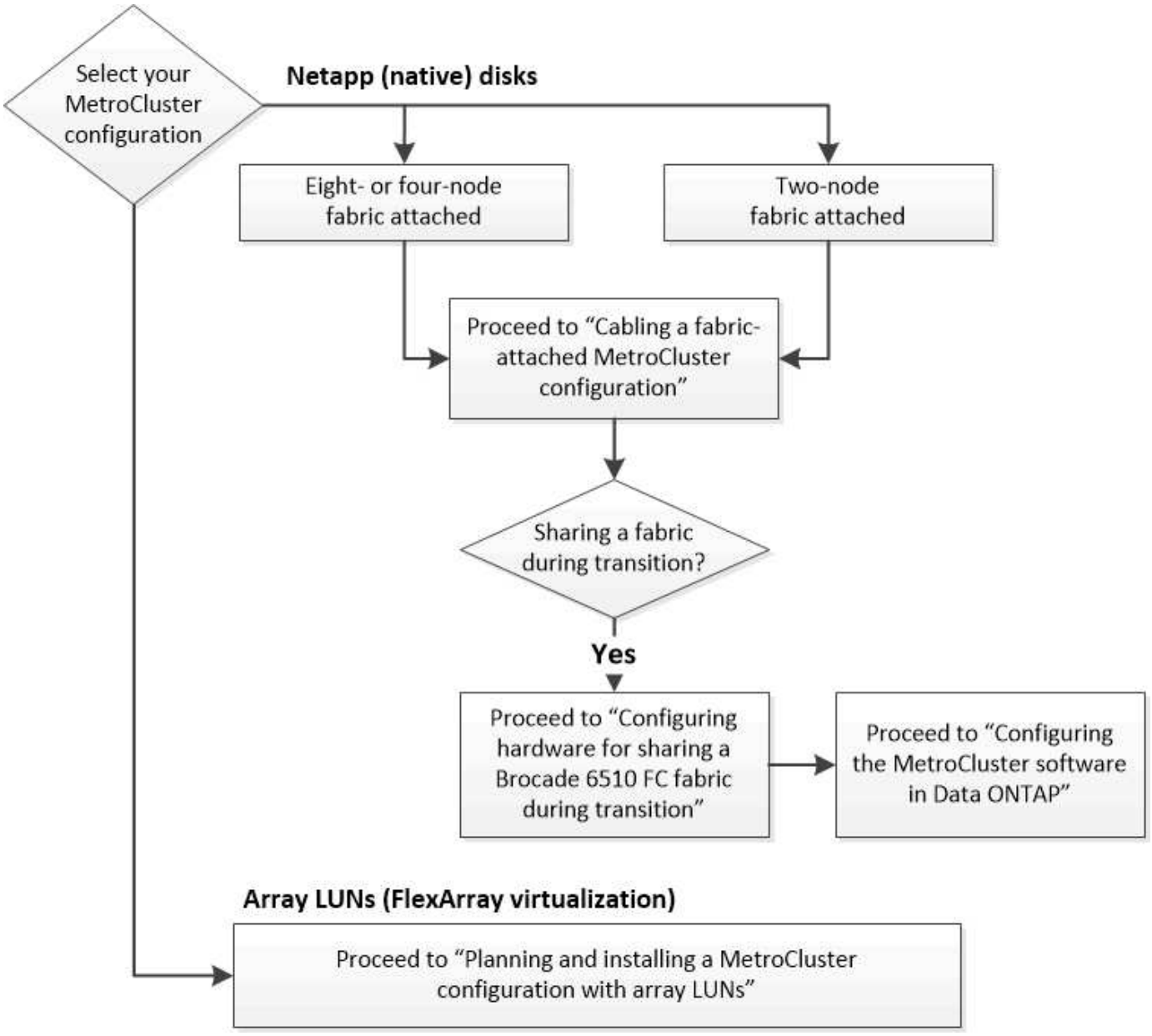
Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o acesso às portas necessárias.

A tabela a seguir mostra o uso da porta TCP/UDP em um firewall externo posicionado entre dois sites do MetroCluster.

Tipo de trânsito	Porta/serviços
Peering de clusters	11104 / TCP 11105 / TCP
Gerente do sistema da ONTAP	443 / TCP
LIFs IP entre clusters do MetroCluster	65200 / TCP 10006 / TCP e UDP
Assistência ao hardware	4444 / TCP

Escolhendo o procedimento de instalação correto para sua configuração

Você deve escolher o procedimento de instalação correto com base no uso de LUNs FlexArray, no número de nós na configuração MetroCluster e se você está compartilhando uma malha de switch FC existente usada por um MetroCluster de malha de 7 modos.



Para este tipo de instalação…	Utilize estes procedimentos…
Configuração conectada à malha com discos NetApp (nativos)	1. "Fazer o cabeamento de uma configuração MetroCluster conectada à malha" 2. "Configurando o software MetroCluster no ONTAP"
Configuração conectada à malha ao compartilhar com uma malha de switch FC existente Isso é suportado apenas como uma configuração temporária com uma configuração de MetroCluster de malha de 7 modos usando os switches Brocade 6510.	1. "Fazer o cabeamento de uma configuração MetroCluster conectada à malha" 2. "Configuração do hardware do MetroCluster para compartilhar uma malha de FC Brocade 6510 de 7 modos durante a transição" 3. "Configurando o software MetroCluster no ONTAP"

Cable uma configuração de MetroCluster conectada à malha

Fazer o cabeamento de uma configuração MetroCluster conectada à malha

Os componentes do MetroCluster devem ser fisicamente instalados, cabeados e configurados em ambos os locais geográficos. As etapas são ligeiramente diferentes para um sistema com compartimentos de disco nativos, em vez de um sistema com LUNs de array.

Partes de uma configuração de Fabric MetroCluster

Partes de uma configuração de Fabric MetroCluster

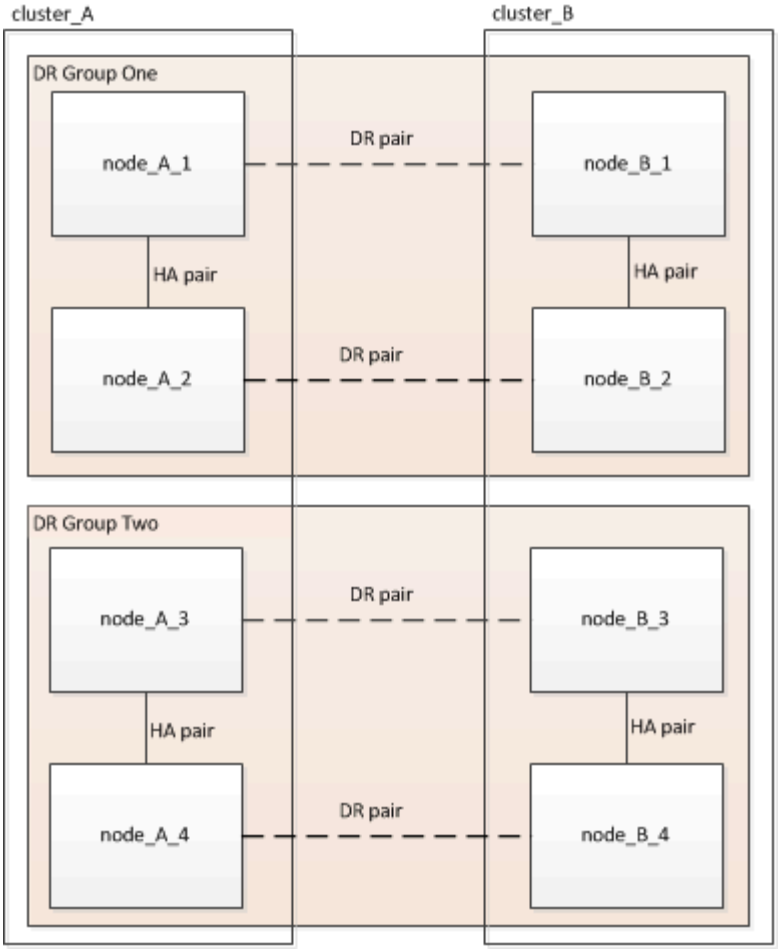
Ao Planejar sua configuração do MetroCluster, você deve entender os componentes de hardware e como eles se interconetam.

Grupos de recuperação de desastres (DR)

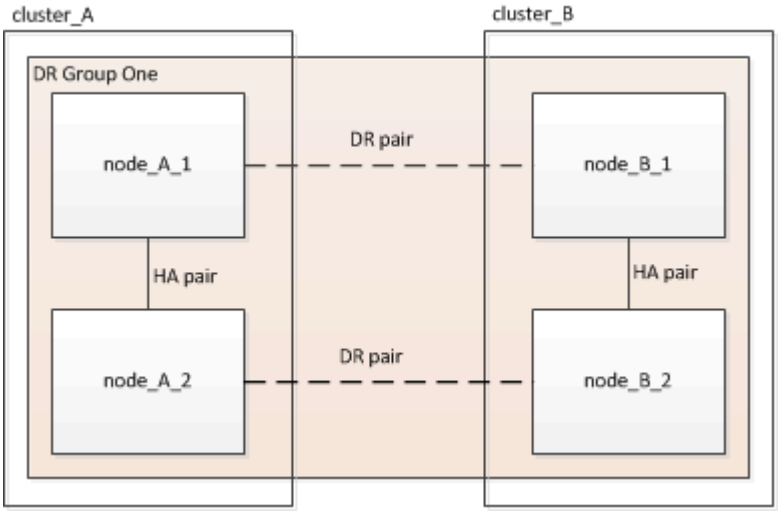
Uma configuração do Fabric MetroCluster consiste em um ou dois grupos de DR, dependendo do número de nós na configuração do MetroCluster. Cada grupo de DR consiste em quatro nós.

- Uma configuração do MetroCluster de oito nós consiste em dois grupos de DR.
- Uma configuração de MetroCluster de quatro nós consiste em um grupo de DR.

A ilustração a seguir mostra a organização de nós em uma configuração de MetroCluster de oito nós:



A ilustração a seguir mostra a organização de nós em uma configuração de MetroCluster de quatro nós:



Principais elementos de hardware

Uma configuração do MetroCluster inclui os seguintes elementos-chave de hardware:

- Controladores de storage

  As controladoras de storage não são conectadas diretamente ao storage, mas conectadas a duas malhas de switches FC redundantes.

- Pontes FC para SAS

  As pontes FC para SAS conectam as stacks de storage SAS aos switches FC, fornecendo uma ponte entre os dois protocolos.

- Switches FC

  Os switches FC fornecem o backbone de longo curso ISL entre os dois locais. Os switches FC fornecem as duas malhas de storage que permitem o espelhamento de dados para os pools de storage remoto.

- Rede de peering de cluster

  A rede de peering de cluster fornece conetividade para espelhamento da configuração do cluster, que inclui a configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.

Configuração de MetroCluster de malha de oito nós

Uma configuração de oito nós consiste em dois clusters, um em cada local geograficamente separado. O cluster_A está localizado no primeiro site do MetroCluster. O cluster_B está localizado no segundo site do MetroCluster. Cada local tem uma pilha de storage SAS. São suportadas stacks de armazenamento adicionais, mas apenas uma é mostrada em cada local. Os pares de HA são configurados como clusters sem switch, sem switches de interconexão de cluster. É suportada uma configuração comutada, mas não é apresentada.

Uma configuração de oito nós inclui as seguintes conexões:

- Conexões FC de cada controlador HBAs e adaptadores FC-VI para cada um dos switches FC
- Uma conexão FC de cada bridge FC para SAS e um switch FC
- Conexões SAS entre cada compartimento SAS e da parte superior e inferior de cada stack até uma ponte FC para SAS
- Uma interconexão de HA entre cada controlador no par de HA local

  Se os controladores suportarem um par de HA de chassi único, a interconexão de HA será interna, ocorrendo através do backplane, o que significa que não é necessária uma interconexão externa.

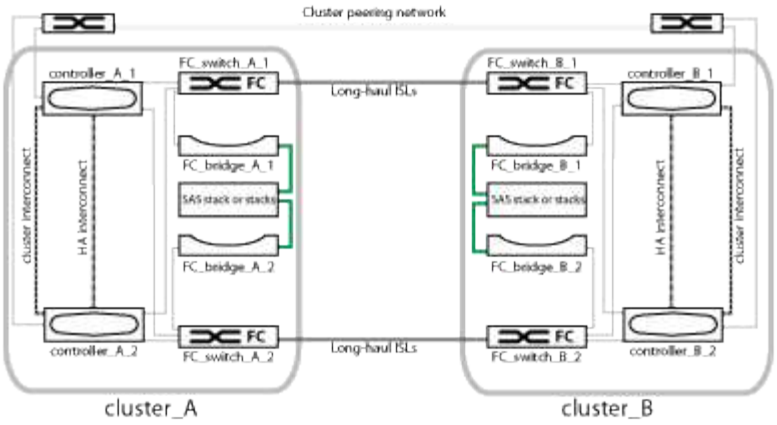
- Conexões Ethernet dos controladores para a rede fornecida pelo cliente que é usada para peering de cluster

  A configuração da SVM é replicada na rede de peering de cluster.

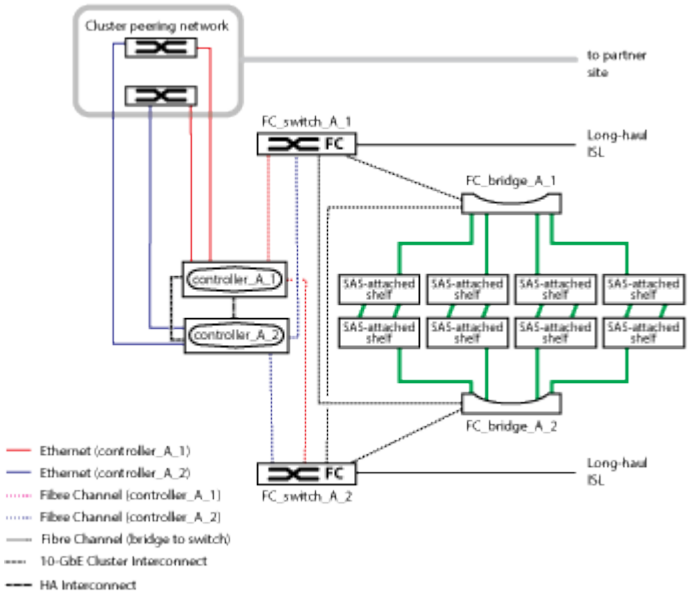
- Uma interconexão de cluster entre cada controlador no cluster local

Configuração de MetroCluster de malha de quatro nós

A ilustração a seguir mostra uma visualização simplificada de uma configuração de MetroCluster de malha de quatro nós. Para algumas conexões, uma única linha representa várias conexões redundantes entre os componentes. As conexões de rede de gerenciamento e dados não são mostradas.

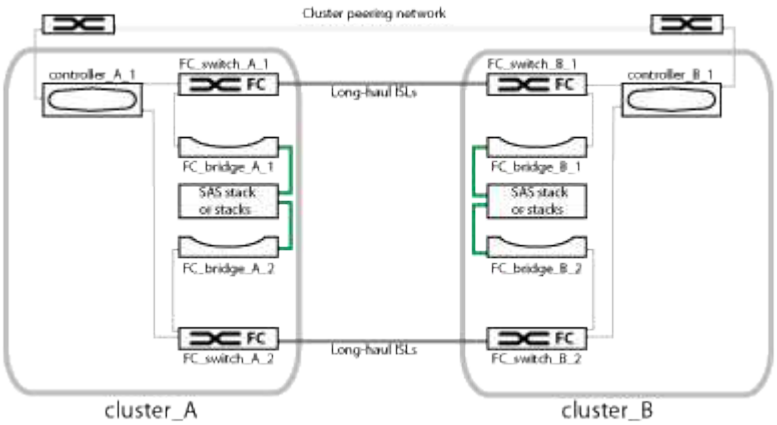


A ilustração a seguir mostra uma visão mais detalhada da conectividade em um único cluster MetroCluster (ambos os clusters têm a mesma configuração):



Configuração de MetroCluster de malha de dois nós

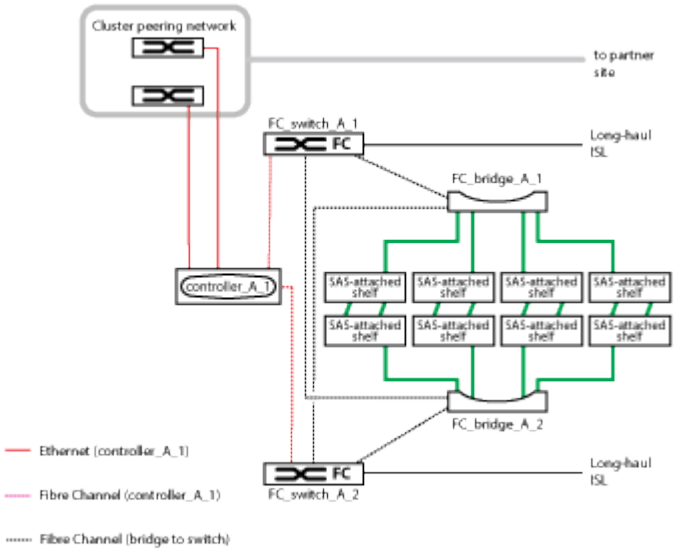
A ilustração a seguir mostra uma visualização simplificada de uma configuração de MetroCluster de malha de dois nós. Para algumas conexões, uma única linha representa várias conexões redundantes entre os componentes. As conexões de rede de gerenciamento e dados não são mostradas.



Uma configuração de dois nós consiste em dois clusters, um em cada local geograficamente separado. O cluster_A está localizado no primeiro site do MetroCluster. O cluster_B está localizado no segundo site do MetroCluster. Cada local tem uma pilha de storage SAS. São suportadas stacks de armazenamento adicionais, mas apenas uma é mostrada em cada local.

Em uma configuração de dois nós, os nós não são configurados como um par de HA.

A ilustração a seguir mostra uma visão mais detalhada da conectividade em um único cluster MetroCluster (ambos os clusters têm a mesma configuração):



Uma configuração de dois nós inclui as seguintes conexões:

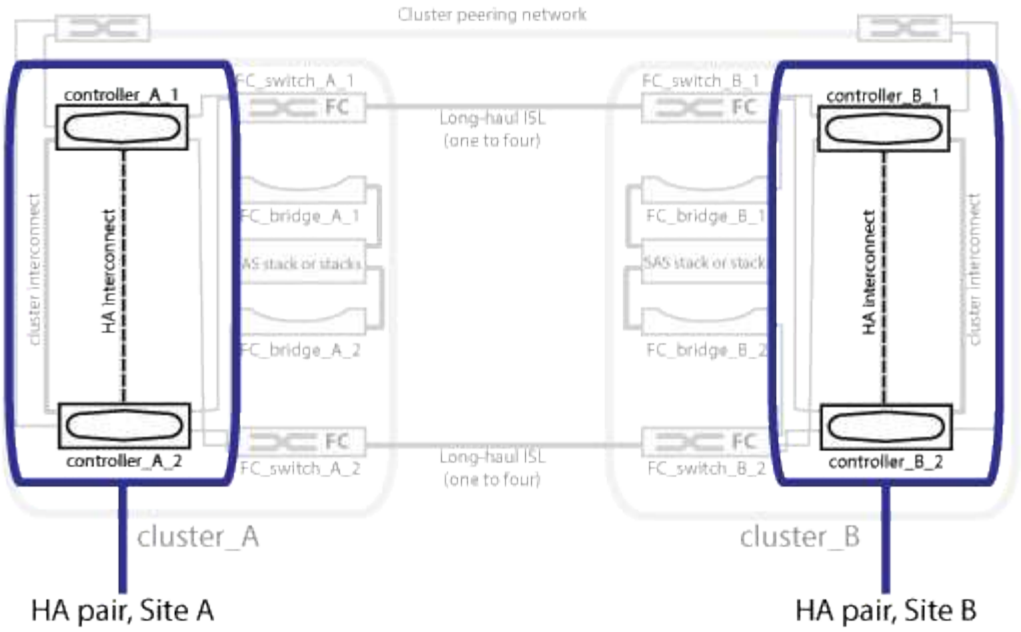
- Conexões FC entre o adaptador FC-VI em cada módulo de controladora
- Conexões FC de HBAs de cada módulo de controladora à ponte FC-para-SAS para cada stack de gaveta SAS
- Conexões SAS entre cada compartimento SAS e da parte superior e inferior de cada stack até uma ponte FC para SAS
- Conexões Ethernet dos controladores para a rede fornecida pelo cliente que é usada para peering de cluster

  A configuração da SVM é replicada na rede de peering de cluster.

Ilustração dos pares de HA locais em uma configuração do MetroCluster

Em configurações de MetroCluster de oito ou quatro nós, cada local consiste em controladores de storage configurados como um ou dois pares de HA. Isso permite redundância local para que, se um controlador de storage falhar, seu parceiro de HA local possa assumir o controle. Essas falhas podem ser tratadas sem uma operação de switchover do MetroCluster.

As operações de failover de HA local e giveback são executadas com os comandos de failover de storage, da mesma maneira que uma configuração que não é MetroCluster.



Informações relacionadas

"Ilustração de pontes FC para SAS redundantes"

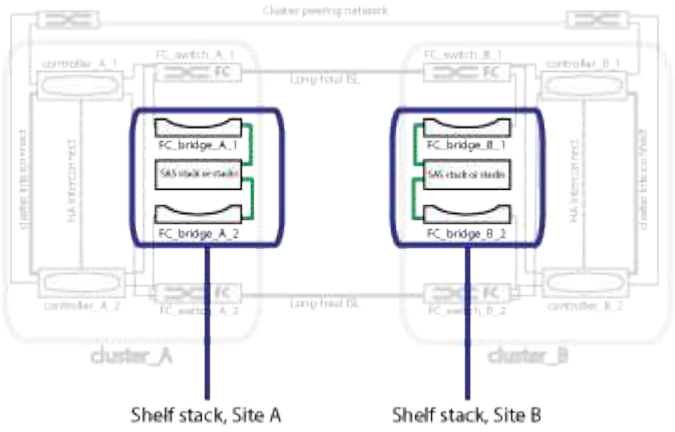
"Malhas de switches FC redundantes"

"Ilustração da rede de peering de cluster"

"Conceitos de ONTAP"

Ilustração de pontes FC para SAS redundantes

As pontes FC para SAS fornecem pontes de protocolo entre os discos conectados a SAS e a malha do switch FC.



Informações relacionadas

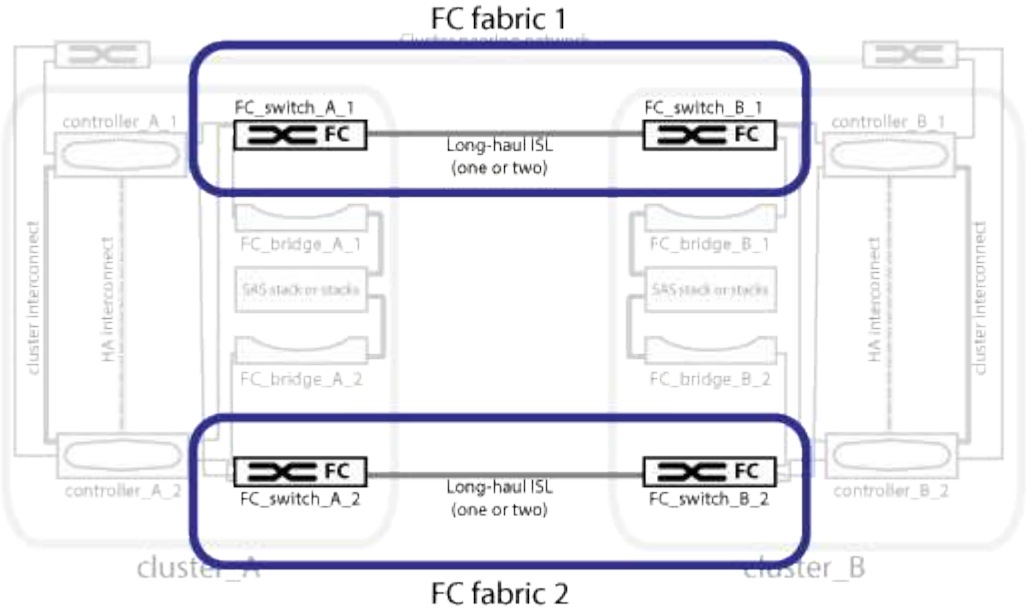
"Ilustração dos pares de HA locais em uma configuração do MetroCluster"

"Malhas de switches FC redundantes"

"Ilustração da rede de peering de cluster"

Malhas de switches FC redundantes

Cada malha de switch inclui links inter-switch (ISLs) que conetam os sites. Os dados são replicados de um site para outro através do ISL. Cada malha de switch deve estar em caminhos físicos diferentes para redundância.



Informações relacionadas

"Ilustração dos pares de HA locais em uma configuração do MetroCluster"

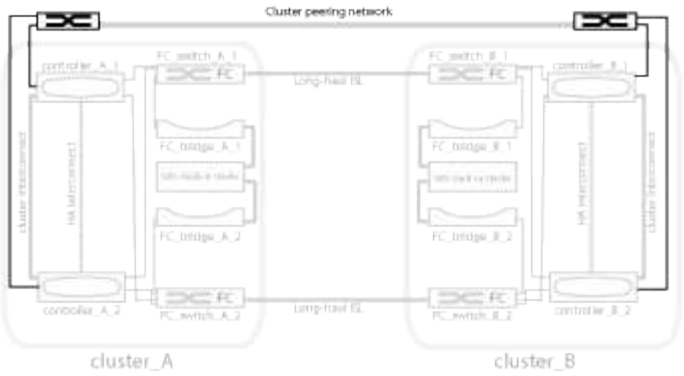
"Ilustração de pontes FC para SAS redundantes"

"Ilustração da rede de peering de cluster"

Ilustração da rede de peering de cluster

Os dois clusters na configuração do MetroCluster são direcionados por meio de uma rede de peering de cluster fornecida pelo cliente. O peering de cluster suporta o espelhamento síncrono de máquinas virtuais de armazenamento (SVMs, anteriormente conhecido como VServers) entre os sites.

As LIFs entre clusters devem ser configuradas em cada nó na configuração do MetroCluster e os clusters devem ser configurados para peering. As portas com os LIFs entre clusters são conetadas à rede de peering de cluster fornecida pelo cliente. A replicação da configuração SVM é realizada por meio dessa rede por meio do Configuration Replication Service.



Informações relacionadas

"Ilustração dos pares de HA locais em uma configuração do MetroCluster"

"Ilustração de pontes FC para SAS redundantes"

"Malhas de switches FC redundantes"

"Configuração expressa de peering de cluster e SVM"

"Considerações para configurar o peering de cluster"

"Cabeamento das conexões de peering de cluster"

"Peering dos clusters"

Componentes e convenções de nomenclatura necessários do MetroCluster FC

Ao Planejar a configuração do MetroCluster FC, você precisa entender os componentes de software e hardware necessários e compatíveis. Para conveniência e clareza, você também deve entender as convenções de nomenclatura usadas para componentes em exemplos ao longo da documentação. Por exemplo, um site é referido como Site A e o outro site é referido como Site B.

Software e hardware suportados

O hardware e o software devem ser compatíveis com a configuração MetroCluster FC.

"NetApp Hardware Universe"

Ao usar sistemas AFF, todos os módulos do controlador na configuração do MetroCluster devem ser configurados como sistemas AFF.

SFPs de onda longa não são suportados nos switches de armazenamento MetroCluster. Para obter uma tabela de SPFs compatíveis, consulte o Relatório técnico da MetroCluster.

Redundância de hardware na configuração MetroCluster FC

Devido à redundância de hardware na configuração MetroCluster FC, há dois de cada componente em cada local. Os sites são arbitrariamente atribuídos às letras A e B e os componentes individuais são arbitrariamente atribuídos aos números 1 e 2.

Requisito para dois clusters ONTAP

A configuração de MetroCluster FC conectada à malha requer dois clusters ONTAP, um em cada local da MetroCluster.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Requisito para quatro switches FC

A configuração MetroCluster FC conectada à malha requer quatro switches FC (modelos Brocade ou Cisco compatíveis).

Os quatro switches formam duas malhas de storage de switch que fornecem o ISL entre cada um dos clusters na configuração MetroCluster FC.

A nomeação deve ser única dentro da configuração do MetroCluster.

Requisito para dois, quatro ou oito módulos de controlador

A configuração MetroCluster FC conectada à malha requer dois, quatro ou oito módulos de controladora.

Em uma configuração de MetroCluster de quatro ou oito nós, os módulos de controladora em cada local formam um ou dois pares de HA. Cada módulo de controladora tem um parceiro de recuperação de desastres no outro local.

Os módulos do controlador devem atender aos seguintes requisitos:

- A nomeação deve ser única dentro da configuração do MetroCluster.
- Todos os módulos do controlador na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.
- Todos os módulos de controladora em um grupo de DR devem ter o mesmo modelo.

  No entanto, em configurações com dois grupos de DR, cada grupo de DR pode consistir em diferentes modelos de módulo de controladora.

- Todos os módulos de controladora em um grupo de DR devem usar a mesma configuração FC-VI.

  Alguns módulos de controladora suportam duas opções de conectividade FC-VI:

  - Portas FC-VI integradas
  - Uma placa FC-VI no slot 1 Uma combinação de um módulo de controladora usando portas FC-VI integradas e outra usando uma placa FC-VI complementar não é compatível. Por exemplo, se um nó usar a configuração FC-VI integrada, todos os outros nós do grupo de DR também precisarão usar a configuração FC-VI integrada.

Nomes de exemplo:

- Local A: Controller_A_1

- Local B: Controller_B_1

Requisito para quatro switches de interconexão de cluster

A configuração de FC MetroCluster conectado à malha requer quatro switches de interconexão de cluster (se você não estiver usando clusters sem switch de dois nós)

Esses switches fornecem comunicação de cluster entre os módulos do controlador em cada cluster. Os switches não são necessários se os módulos do controlador em cada local forem configurados como um cluster sem switch de dois nós.

Requisito para pontes FC para SAS

A configuração de FC MetroCluster conectado à malha requer um par de pontes FC para SAS para cada grupo de stack de gavetas SAS.

> As bridges FibreBridge 6500N não são suportadas em configurações que executam o ONTAP 9.8 e posterior.

- As bridges FibreBridge 7600N ou 7500N suportam até quatro stacks SAS.
- Cada stack pode usar diferentes modelos de IOM.

  Uma combinação de IOM12 módulos e IOM3 módulos não é suportada na mesma pilha de storage. Uma combinação de IOM12 módulos e IOM6 módulos é compatível com a mesma pilha de storage se o sistema estiver executando uma versão compatível do ONTAP.

  Os módulos IOM suportados dependem da versão do ONTAP que você está executando.

- A nomeação deve ser única dentro da configuração do MetroCluster.

Os nomes sugeridos usados como exemplos nesta documentação identificam o módulo do controlador e a pilha à qual a ponte se coneta, conforme mostrado abaixo.

Requisitos de pool e unidade (mínimo suportado)

São recomendadas oito gavetas de disco SAS (quatro gavetas em cada local) para permitir a propriedade de disco por compartimento.

A configuração do MetroCluster requer a configuração mínima em cada local:

- Cada nó tem pelo menos um pool local e um pool remoto no local.

  Por exemplo, em uma configuração de MetroCluster de quatro nós com dois nós em cada local, quatro pools são necessários em cada local.

- Pelo menos sete unidades em cada pool.

  Em uma configuração de MetroCluster de quatro nós com um único agregado de dados espelhados por nó, a configuração mínima requer 24 discos no local.

Em uma configuração mínima suportada, cada pool tem o seguinte layout de unidade:

- Três unidades raiz

- Três unidades de dados
- Uma unidade sobressalente

Em uma configuração mínima com suporte, pelo menos um compartimento é necessário por local.

As configurações do MetroCluster são compatíveis com RAID-DP e RAID4.

Considerações sobre o local da unidade para compartimentos parcialmente preenchidos

Para a atribuição automática correta de unidades ao usar compartimentos com metade população (12 unidades em um compartimento de 24 unidades), as unidades devem estar localizadas nos slots 0-5 e 18-23.

Em uma configuração com um compartimento parcialmente preenchido, as unidades precisam ser distribuídas uniformemente nos quatro quadrantes da gaveta.

Misturando módulos IOM12 e IOM 6 em uma pilha

Sua versão do ONTAP deve suportar a mistura de prateleiras. Consulte a ferramenta de Matriz de interoperabilidade (IMT) para ver se a sua versão do ONTAP suporta a mistura de prateleiras. "IMT"

Para obter mais detalhes sobre a mistura de prateleiras, consulte: "Gavetas de adição dinâmica com IOM12 módulos para uma stack de gavetas com IOM6 módulos"

Convenções de nomenclatura de ponte

As pontes usam o seguinte exemplo de nomenclatura:

```
bridge_site_stack grouplocation in pair
```

Esta parte do nome…	Identifica o…	Valores possíveis…
local	Local no qual o par de pontes reside fisicamente.	A ou B
grupo de pilha	Número do grupo de pilha ao qual o par de ponte se coneta. FibreBridge 7600N ou 7500N bridges suportam até quatro stacks no grupo stack. O grupo de stack não pode conter mais de 10 gavetas de storage.	1, 2, etc.
localização em par	Ponte dentro do par de ponte.Um par de pontes se coneta a um grupo de pilha específico.	a ou b

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b

- bridge_B_1a
- bridge_B_1b

Planilhas de configuração para switches FC e bridges FC para SAS

Antes de começar a configurar os sites do MetroCluster, você pode usar as seguintes planilhas para gravar as informações do site:

"Coloque Uma Planilha no local"

"Folha de trabalho do local B."

Instale e faça o cabo dos componentes do MetroCluster

Colocar em pilha os componentes de hardware

Se você não recebeu o equipamento já instalado em armários, você deve colocar os componentes em rack.

Sobre esta tarefa

Esta tarefa tem de ser executada em ambos os sites da MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   O espaço em rack depende do modelo de plataforma dos módulos do controlador, dos tipos de switch e do número de pilhas de compartimento de disco na sua configuração.

2. Aterre-se corretamente.
3. Instale os módulos do controlador no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Instale os switches FC no rack ou gabinete.
5. Instale as gavetas de disco, ligue-as e, em seguida, defina as IDs das gaveta.
   - É necessário desligar cada compartimento de disco.
   - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
6. Instalar cada ponte FC para SAS:

   a. Fixe os suportes "L" na parte frontal da ponte à frente do rack (montagem embutida) com os quatro parafusos.

      As aberturas nos suportes da ponte "L" estão em conformidade com o padrão de rack ETA-310-X para racks de 19 polegadas (482,6 mm).

      O *ATTO FibreBridge Installation and Operation Manual* do seu modelo de ponte contém mais informações e uma ilustração da instalação.

Para um acesso adequado ao espaço da porta e manutenção da FRU, você deve deixar espaço 1UD abaixo do par de pontes e cobrir esse espaço com um painel de supressão sem ferramentas.

b. Conete cada ponte a uma fonte de alimentação que forneça um aterramento adequado.

c. Ligue cada ponte.

Para obter a resiliência máxima, as bridges que estão conectadas à mesma stack de shelves de disco devem ser conectadas a diferentes fontes de energia.

O LED bridge Ready pode demorar até 30 segundos a acender, indicando que a ponte concluiu a sequência de autoteste de ativação.

Faça o cabeamento das portas FC-VI e HBA do novo módulo de controladora aos switches FC

As portas FC-VI e HBAs (adaptadores de barramento do host) devem ser cabeadas para os switches FC do local em cada módulo de controladora na configuração do MetroCluster.

Passos

1. Faça o cabeamento das portas FC-VI e das portas HBA, usando a tabela para sua configuração e modelo de switch.
   - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"
   - "Atribuições de portas para switches FC ao usar sistemas AFF A900"
   - "Atribuições de portas para sistemas que usam duas portas de iniciador"

Fazer o cabeamento das ISLs entre os locais do MetroCluster

É necessário conetar os switches FC em cada local por meio dos links interswitches (ISLs) de fibra ótica para formar as malhas de switch que conetam os componentes do MetroCluster.

Sobre esta tarefa

Isso deve ser feito para ambos os tecidos de troca.

Passos

1. Conete os switches FC em cada local a todos os ISLs, usando o cabeamento na tabela que corresponde à configuração e ao modelo de switch.
   - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Informações relacionadas

"Considerações para ISLs"

Atribuições de portas para sistemas que usam duas portas de iniciador

Você pode configurar sistemas FAS8020, AFF8020, FAS8200 e AFF A300 usando uma única porta de iniciador para cada malha e duas portas de iniciador para cada controladora.

Você pode seguir o cabeamento da ponte FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2). Em vez de usar quatro iniciadores, conete apenas dois iniciadores e deixe os outros dois conetados à porta do switch vazios.

Se o zoneamento for executado manualmente, siga o zoneamento usado para uma ponte FibreBridge 7500N ou 7600N usando uma porta FC (FC1 ou FC2). Nesse cenário, uma porta iniciador em vez de duas é adicionada a cada membro da zona por malha.

Você pode alterar o zoneamento ou executar uma atualização de um FibreBridge 6500N para um FibreBridge 7500N usando o procedimento em "Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N".

A tabela a seguir mostra as atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior.

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)			
MetroCluster 1 ou Grupo DR 1			
Componente	**Porto**	**Brocade switch modelos 6505, 6510, 6520, 7840, G620, G610 e DCX 8510-8**	
		* Coneta-se ao switch FC…*	* Coneta-se à porta do switch…*
controller_x_1	Porta a FC-VI	1	0
	Porta FC-VI b	2	0
	Porta FC-VI c	1	1
	Porta d. FC-VI	2	1
	HBA porta a	1	2
	Porta HBA b	2	2
	Porta HBA c	-	-
	Porta d. HBA	-	-
Pilha 1	bridge_x_1a	1	8
bridge_x_1b	2	8	Empilha y
bridge_x_ya	1	11	ponte_x_yb

A tabela a seguir mostra as atribuições de portas para switches FC ao usar o ONTAP 9.0.

Configuração de dois nós MetroCluster

Componente	Porto	Brocade 6505, 6510 ou DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta a FC-VI	0	-
Porta FC-VI b	-	0	HBA porta a
1	-	Porta HBA b	-
1	Porta HBA c	2	-

Atribuições de portas para switches FC ao usar o ONTAP 9.1 ou posterior

Você precisa verificar se está usando as atribuições de portas especificadas quando você faz o cabeamento dos switches FC usando o ONTAP 9.1 e posterior.

As portas que não são usadas para anexar portas do iniciador, portas FC-VI ou ISLs podem ser reconfiguradas para agir como portas de storage. No entanto, se os RCFs suportados estiverem sendo usados, o zoneamento deve ser alterado em conformidade.

Se os RCFs suportados forem usados, as portas ISL podem não se conetar às mesmas portas mostradas e podem precisar ser reconfiguradas manualmente.

Se você configurou seus switches usando as atribuições de portas do ONTAP 9, poderá continuar a usar as atribuições mais antigas. No entanto, novas configurações que executam o ONTAP 9.1 ou versões posteriores devem usar as atribuições de portas mostradas aqui.

Diretrizes gerais de cabeamento

Você deve estar ciente das seguintes diretrizes ao usar as tabelas de cabeamento:

- Os switches Brocade e Cisco usam numeração de portas diferente:
  - Nos switches Brocade, a primeira porta é numerada 0.
  - Nos switches Cisco, a primeira porta é numerada 1.
- O cabeamento é o mesmo para cada switch FC na malha do switch.
- Os sistemas de storage AFF A300 e FAS8200 podem ser solicitados com uma das duas opções de conectividade FC-VI:
  - Portas integradas 0e e 0f configuradas no modo FC-VI.
  - Portas 1a e 1b em uma placa FC-VI no slot 1.
- Os sistemas de storage AFF A700 e FAS9000 exigem quatro portas FC-VI. As tabelas a seguir mostram o cabeamento dos switches FC com quatro portas FC-VI em cada controladora, exceto o switch Cisco 9250i.

  Para outros sistemas de armazenamento, use o cabeamento mostrado nas tabelas, mas ignore o cabeamento das portas FC-VI c e d.

  Você pode deixar essas portas vazias.

- Os sistemas de storage AFF A400 e FAS8300 usam as portas 2a e 2b para conectividade FC-VI.
- Se você tiver duas configurações do MetroCluster compartilhando ISLs, use as mesmas atribuições de porta que aquela para um cabeamento MetroCluster de oito nós.

  O número de ISLs que você faz a cabo pode variar dependendo dos requisitos do local.

  Consulte a secção sobre considerações ISL.

Uso de porta Brocade para controladores em uma configuração MetroCluster executando o ONTAP 9.1 ou posterior

As tabelas a seguir mostram o uso de portas nos switches Brocade. As tabelas mostram a configuração máxima suportada, com oito módulos de controlador em dois grupos de DR. Para configurações menores, ignore as linhas dos módulos adicionais do controlador. Observe que oito ISLs são suportadas apenas nos switches Brocade 6510, Brocade DCX 8510-8, G620, G630, G620-1, G630-1 e G720.

- O uso de porta para os switches Brocade 6505 e Brocade G610 em uma configuração de MetroCluster de oito nós não é mostrado. Devido ao número limitado de portas, as atribuições de portas devem ser feitas de acordo com o modelo do módulo do controlador e o número de ISLs e pares de pontes em uso.
- O switch Brocade DCX 8510-8 pode usar o mesmo layout de porta que o switch 6510 ***or*** o switch 7840.

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)				
MetroCluster 1 ou Grupo de RD 1				
Componente	Porta	Interrutor Brocade modelos 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 e DCX 8510-8		Interrutor Brocade modelo G720
		Liga ao interrutor FC…	Liga à porta do switch…	Liga à porta do switch…
controller_x_1	Porta a FC-VI	1	0	0
Porta FC-VI b	2	0	0	Porta FC-VI c
1	1	1	Porta d. FC-VI	2
1	1	HBA porta a	1	2
8	Porta HBA b	2	2	8
Porta HBA c	1	3	9	Porta d. HBA
2	3	9	controller_x_2	Porta a FC-VI
1	4	4	Porta FC-VI b	2
4	4	Porta FC-VI c	1	5

5	Porta d. FC-VI	2	5	5
HBA porta a	1	6	12	Porta HBA b
2	6	12	Porta HBA c	1
7	13	Porta d. HBA	2	7

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)				
MetroCluster 1 ou Grupo de RD 1				
Componente	Porta	Interrutor Brocade modelos 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 e DCX 8510-8		Interrutor Brocade modelo G720
		Liga ao interrutor FC…	Liga à porta do switch…	Liga à porta do switch…
Pilha 1	bridge_x_1a	1	8	10
bridge_x_1b	2	8	10	Pilha 2
bridge_x_2a	1	9	11	bridge_x_2b
2	9	11	Pilha 3	bridge_x_3a
1	10	14	bridge_x_4b	2
10	14	Empilha y	bridge_x_ya	1
11	15	ponte_x_yb	2	11

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)							
MetroCluster 2 ou Grupo de RD 2							
			Modelo de interrutor Brocade				
Componente	Porta	Liga ao FC_switch…	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720
controller_x_3	Porta a FC-VI	1	24	48	12	18	18
Porta FC-VI b	2	24	48	12	18	18	Porta FC-VI c

1	25	49	13	19	19	Porta d. FC-VI	2
25	49	13	19	19	HBA porta a	1	26
50	14	24	26	Porta HBA b	2	26	50
14	24	26	Porta HBA c	1	27	51	15
25	27	Porta d. HBA	2	27	51	15	25
27	controller_x_4	Porta a FC-VI	1	28	52	16	22
22	Porta FC-VI b	2	28	52	16	22	22
Porta FC-VI c	1	29	53	17	23	23	Porta d. FC-VI
2	29	53	17	23	23	HBA porta a	1
30	54	18	28	30	Porta HBA b	2	30
54	18	28	30	Porta HBA c	1	31	55
19	29	31	Porta d. HBA	2	32	55	19
29	31	Pilha 1	bridge_x_51 a	1	32	56	20
26	32	bridge_x_51 b	2	32	56	20	26
32	Pilha 2	bridge_x_52 a	1	33	57	21	27
33	bridge_x_52 b	2	33	57	21	27	33
Pilha 3	bridge_x_53 a	1	34	58	22	30	34

bridge_x_54b	2	34	58	22	30	34	Empilha y
bridge_x_ya	1	35	59	23	31	35	ponte_x_yb

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)					
MetroCluster 1 ou Grupo de RD 1					
Componente		Porta	Interrutor Brocade modelos 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 e DCX 8510-8		Interrutor Brocade G720
			Liga ao FC_switch…	Liga à porta do switch…	Liga à porta do switch…
Pilha 1	bridge_x_1a	FC1	1	8	10
FC2	2	8	10	bridge_x_1B	FC1
1	9	11	FC2	2	9
11	Pilha 2	bridge_x_2a	FC1	1	10
14	FC2	2	10	14	bridge_x_2B
FC1	1	11	15	FC2	2
11	15	Pilha 3	bridge_x_3a	FC1	1
12*	16	FC2	2	12*	16
bridge_x_3B	FC1	1	13*	17	FC2
2	13*	17	Empilha y	bridge_x_ya	FC1
1	14*	20	FC2	2	14*
20	ponte_x_yb	FC1	1	15*	21

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)
MetroCluster 2 ou Grupo de RD 2

Componente		Porta	Modelo de interrutor Brocade					
			Liga ao FC_switch …	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720
controller_x_3	Porta a FC-VI	1	24	48	12	18	18	Porta FC-VI b
2	24	48	12	18	18	Porta FC-VI c	1	25
49	13	19	19	Porta d. FC-VI	2	25	49	13
19	19	HBA porta a	1	26	50	14	24	26
Porta HBA b	2	26	50	14	24	26	Porta HBA c	1
27	51	15	25	27	Porta d. HBA	2	27	51
15	25	27	controller_x_4	Porta a FC-VI	1	28	52	16
22	22	Porta FC-VI b	2	28	52	16	22	22
Porta FC-VI c	1	29	53	17	23	23	Porta d. FC-VI	2
29	53	17	23	23	HBA porta a	1	30	54
18	28	30	Porta HBA b	2	30	54	18	28
30	Porta HBA c	1	31	55	19	29	31	Porta d. HBA
2	31	55	19	29	31	Pilha 1	bridge_x_51a	FC1
1	32	56	20	26	32	FC2	2	32

56	20	26	32	bridge_x_51b	FC1	1	33	57
21	27	33	FC2	2	33	57	21	27
33	Pilha 2	bridge_x_52a	FC1	1	34	58	22	30
34	FC2	2	34	58	22	30	34	bridge_x_52b
FC1	1	35	59	23	31	35	FC2	2
35	59	23	31	35	Pilha 3	bridge_x_53a	FC1	1
36	60	-	32	36	FC2	2	36	60
-	32	36	bridge_x_53b	FC1	1	37	61	-
33	37	FC2	2	37	61	-	33	37
Empilha y	bridge_x_5ya	FC1	1	38	62	-	34	38
FC2	2	38	62	-	34	38	bridge_x_5yb	FC1
1	39	63	-	35	39	FC2	2	39

Uso de porta Brocade para ISLs em uma configuração MetroCluster executando o ONTAP 9.1 ou posterior

A tabela a seguir mostra o uso da porta ISL para os switches Brocade.

Os sistemas AFF A700 ou FAS9000 suportam até oito ISLs para melhorar o desempenho. Oito ISLs são suportadas nos switches Brocade 6510 e G620.

Modelo do interrutor	Porta de ISL	Porta do switch
Brocade 6520	Porta ISL 1	23
Porta ISL 2	47	Porta ISL 3
71	Porta ISL 4	95

Brocade 6505	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46
Porta ISL 8	47	Brocade 7810
Porta ISL 1	GE2 Gbps (10 Gbps)	Porta ISL 2
ge3 Gbps (10 Gbps)	Porta ISL 3	ge4 Gbps (10 Gbps)
Porta ISL 4	ge5 Gbps (10 Gbps)	Porta ISL 5
GE6 Gbps (10 Gbps)	Porta ISL 6	ge7 Gbps (10 Gbps)
Brocade 7840 **Nota**: O switch Brocade 7840 suporta duas portas VE de 40 Gbps ou até quatro portas VE de 10 Gbps por switch para a criação de ISLs FCIP.	Porta ISL 1	ge0 Gbps (40 Gbps) ou GE2 Gbps (10 Gbps)
Porta ISL 2	ge1 Gbps (40 Gbps) ou ge3 Gbps (10 Gbps)	Porta ISL 3
ge10 Gbps (10 Gbps)	Porta ISL 4	ge11 Gbps (10 Gbps)
Brocade G610	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23

Brocade G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46

Uso de porta Cisco para controladores em uma configuração MetroCluster executando o ONTAP 9.4 ou posterior

As tabelas mostram o máximo de configurações suportadas, com oito módulos de controladora em dois grupos de DR. Para configurações menores, ignore as linhas dos módulos adicionais do controlador.

Para o Cisco 9132T, Uso da porta Cisco 9132T em uma configuração MetroCluster executando o ONTAP 9.4 ou posteriorconsulte .

Cisco 9396S			
Componente	Porta	Interrutor 1	Interrutor 2
controller_x_1	Porta a FC-VI	1	-
Porta FC-VI b	-	1	Porta FC-VI c
2	-	Porta d. FC-VI	-
2	HBA porta a	3	-
Porta HBA b	-	3	Porta HBA c
4	-	Porta d. HBA	-
4	controller_x_2	Porta a FC-VI	5
-	Porta FC-VI b	-	5
Porta FC-VI c	6	-	Porta d. FC-VI
-	6	HBA porta a	7
-	Porta HBA b	-	7
Porta HBA c	8		Porta d. HBA

-	8	controller_x_3	Porta a FC-VI
49		Porta FC-VI b	-
49	Porta FC-VI c	50	-
Porta d. FC-VI	-	50	HBA porta a
51	-	Porta HBA b	-
51	Porta HBA c	52	
Porta d. HBA	-	52	controller_x_4
Porta a FC-VI	53	-	Porta FC-VI b
-	53	Porta FC-VI c	54
-	Porta d. FC-VI	-	54
HBA porta a	55	-	Porta HBA b
-	55	Porta HBA c	56
-	Porta d. HBA	-	56

Cisco 9148S			
Componente	Porta	Interrutor 1	Interrutor 2
controller_x_1	Porta a FC-VI	1	
Porta FC-VI b	-	1	Porta FC-VI c
2	-	Porta d. FC-VI	-
2	HBA porta a	3	-
Porta HBA b	-	3	Porta HBA c
4	-	Porta d. HBA	-
4	controller_x_2	Porta a FC-VI	5
-	Porta FC-VI b	-	5

Porta FC-VI c	6	-	Porta d. FC-VI
-	6	HBA porta a	7
-	Porta HBA b	-	7
Porta HBA c	8	-	Porta d. HBA
-	8	controller_x_3	Porta a FC-VI
25		Porta FC-VI b	-
25	Porta FC-VI c	26	-
Porta d. FC-VI	-	26	HBA porta a
27	-	Porta HBA b	-
27	Porta HBA c	28	-
Porta d. HBA	-	28	controller_x_4
Porta a FC-VI	29	-	Porta FC-VI b
-	29	Porta FC-VI c	30
-	Porta d. FC-VI	-	30
HBA porta a	31	-	Porta HBA b
-	31	Porta HBA c	32
-	Porta d. HBA	-	32

A tabela a seguir mostra sistemas com duas portas FC-VI. Os sistemas AFF A700 e FAS9000 têm quatro portas FC-VI (a, b, c e d). Se estiver usando um sistema AFF A700 ou FAS9000, as atribuições de portas se movem em uma posição. Por exemplo, as portas FC-VI c e d vão para a porta do switch 2 e as portas HBA a e b vão para a porta do switch 3.

Cisco 9250i Nota: O switch Cisco 9250i não é compatível com configurações MetroCluster de oito nós.			
Componente	Porta	Interrutor 1	Interrutor 2
controller_x_1	Porta a FC-VI	1	-

Porta FC-VI b	-	1	HBA porta a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta d. HBA	-	3	controller_x_2
Porta a FC-VI	4	-	Porta FC-VI b
-	4	HBA porta a	5
-	Porta HBA b	-	5
Porta HBA c	6	-	Porta d. HBA
-	6	controller_x_3	Porta a FC-VI
7	-	Porta FC-VI b	-
7	HBA porta a	8	-
Porta HBA b	-	8	Porta HBA c
9	-	Porta d. HBA	-
9	controller_x_4	Porta a FC-VI	10
-	Porta FC-VI b	-	10
HBA porta a	11	-	Porta HBA b
-	11	Porta HBA c	13
-	Porta d. HBA	-	13

Uso de porta Cisco para pontes FC para SAS em uma configuração do MetroCluster executando o ONTAP 9.1 ou posterior

Cisco 9396S			
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Interrutor 1	Interrutor 2
bridge_x_1a	FC1	9	-

FC2	-	9	bridge_x_1b
FC1	10	-	FC2
-	10	bridge_x_2a	FC1
11	-	FC2	-
11	bridge_x_2b	FC1	12
-	FC2	-	12
bridge_x_3a	FC1	13	-
FC2	-	13	bridge_x_3b
FC1	14	-	FC2
-	14	bridge_x_4a	FC1
15	-	FC2	-
15	bridge_x_4b	FC1	16
-	FC2	-	16

Pontes adicionais podem ser anexadas usando as portas 17 a 40 e 57 a 88 seguindo o mesmo padrão.

Cisco 9148S			
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Interrutor 1	Interrutor 2
bridge_x_1a	FC1	9	-
FC2	-	9	bridge_x_1b
FC1	10	-	FC2
-	10	bridge_x_2a	FC1
11	-	FC2	-
11	bridge_x_2b	FC1	12

-	FC2	-	12
bridge_x_3a	FC1	13	-
FC2	-	13	bridge_x_3b
FC1	14	-	FC2
-	14	bridge_x_4a	FC1
15	-	FC2	-
15	bridge_x_4b	FC1	16
-	FC2	-	16

Bridges adicionais para um segundo grupo de DR ou segunda configuração de MetroCluster podem ser conetadas usando as portas 33 a 40 seguindo o mesmo padrão.

Cisco 9250i			
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Interrutor 1	Interrutor 2
bridge_x_1a	FC1	14	-
FC2	-	14	bridge_x_1b
FC1	15	-	FC2
-	15	bridge_x_2a	FC1
17	-	FC2	-
17	bridge_x_2b	FC1	18
-	FC2	-	18
bridge_x_3a	FC1	19	-
FC2	-	19	bridge_x_3b
FC1	21	-	FC2
-	21	bridge_x_4a	FC1

22	-	FC2	-
22	bridge_x_4b	FC1	23
-	FC2	-	23

Bridges adicionais para um segundo grupo de DR ou segunda configuração de MetroCluster podem ser conetadas usando as portas 25 a 48 seguindo o mesmo padrão.

As tabelas a seguir mostram o uso da porta de ponte ao usar pontes FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2). Para pontes FibreBridge 7500N ou 7600N usando uma porta FC, FC1 ou FC2 podem ser cabeados para a porta indicada como FC1. Pontes adicionais podem ser anexadas usando as portas 25-48.

FibreBridge 7500N ou 7600N pontes usando uma porta FC			
FibreBridge 7500N ou 7600N usando uma porta FC	Porta	Cisco 9396S	
		Interrutor 1	Interrutor 2
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15

bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

Pontes adicionais podem ser anexadas usando as portas 17 a 40 e 57 a 88 seguindo o mesmo padrão.

FibreBridge 7500N ou 7600N pontes usando uma porta FC			
Ponte	Porta	Cisco 9148S	
		Interrutor 1	Interrutor 2
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

Bridges adicionais para um segundo grupo de DR ou segunda configuração de MetroCluster podem ser conetadas usando as portas 25 a 48 seguindo o mesmo padrão.

Cisco 9250i			
FibreBridge 7500N ou 7600N usando uma porta FC	Porta	Interrutor 1	Interrutor 2
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23

Pontes adicionais podem ser anexadas usando as portas 25 a 48 seguindo o mesmo padrão.

Uso de porta Cisco para ISLs em uma configuração de oito nós em uma configuração MetroCluster executando o ONTAP 9.1 ou posterior

A tabela a seguir mostra o uso da porta ISL. O uso da porta ISL é o mesmo em todos os switches na configuração.

Para o Cisco 9132T, Uso da porta ISL para Cisco 9132T em uma configuração MetroCluster executando o ONTAP 9.1 ou posteriorconsulte .

Modelo do interrutor	Porta de ISL	Porta do switch
Cisco 9396S	ISL 1	44
ISL 2	48	ISL 3
92	ISL 4	96
Cisco 9250i com licença de 24 portas	ISL 1	12
ISL 2	16	ISL 3
20	ISL 4	24
Cisco 9148S	ISL 1	20
ISL 2	24	ISL 3
44	ISL 4	48

Uso da porta Cisco 9132T nas configurações de quatro nós e oito nós do MetroCluster executando o ONTAP 9.4 e posterior

As tabelas a seguir mostram o uso da porta em um switch Cisco 9132T. As tabelas mostram o máximo de configurações suportadas com quatro e oito módulos de controladores em dois grupos de DR.

Para configurações de oito nós, você deve executar o zoneamento manualmente porque os RCFs não são fornecidos.

Cisco 9132T com 1x LEM			
MetroCluster 1 ou Grupo de RD 1			
			Quatro nós
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Liga ao FC_switch…	9132T (1x LEM)
bridge_x_1a	FC1	1	LEM1-13
FC2	2	LEM1-13	bridge_x_1b
FC1	1	LEM1-14	FC2

Apenas uma (1) pilha de ponte é suportada usando 9132T switches com 1x módulo LEM.

Cisco 9132T com 2x LEM e um grupo de MetroCluster ou DR de quatro nós			
MetroCluster 1 ou Grupo de RD 1			
			Quatro nós
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Liga ao FC_switch…	9132T (2x LEM)
bridge_x_1a	FC1	1	LEM1-13
FC2	2	LEM1-13	bridge_x_1b
FC1	1	LEM1-14	FC2
2	LEM1-14	bridge_x_2a	FC1
1	LEM1-15	FC2	2
LEM1-15	bridge_x_2b	FC1	1
LEM1-16	FC2	2	LEM1-16
bridge_x_3a	FC1	1	LEM2-1
FC2	2	LEM2-1	bridge_x_3b
FC1	1	LEM2-2	FC2
2	LEM2-2	bridge_x_ya	FC1
1	LEM2-3	FC2	2
LEM2-3	ponte_x_yb	FC1	1
LEM2-4	FC2	2	LEM2-4

Em configurações de quatro nós, você pode fazer o cabeamento de pontes adicionais às portas LEM2-5 a LEM2-8 em switches 9132T com 2x LEMs.

Cisco 9132T com dois Metroclusters de quatro nós ou um MetroCluster de oito nós com dois grupos de DR			
MetroCluster 1 ou Grupo de RD 1			
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Liga ao FC_switch…	9132T (2x LEM)

bridge_x_1a	FC1	1	LEM1-9
FC2	2	LEM1-9	bridge_x_1b
FC1	1	LEM1-10	FC2
2	LEM1-10	bridge_x_2a	FC1
1	LEM1-11	FC2	2
LEM1-11	bridge_x_2b	FC1	1
LEM1-12	FC2	2	LEM1-12
MetroCluster 2 ou Grupo de RD 2			
FibreBridge 7500N ou 7600N usando duas portas FC	Porta	Liga ao FC_switch…	9132T (2x LEM)
bridge_x_3a	FC1	1	LEM2-9
FC2	2	LEM2-9	bridge_x_3b
FC1	1	LEM2-10	FC2
2	LEM2-10	bridge_x_ya	FC1
1	LEM2-11	FC2	2
LEM2-11	ponte_x_yb	FC1	1
LEM2-12	FC2	2	LEM2-12

Em configurações de oito nós, você pode fazer o cabeamento de pontes adicionais às portas LEM2-13 a LEM2-16 em switches 9132T com 2x LEMs.

Uso de porta Cisco 9132T para ISLs em configurações de quatro e oito nós em uma configuração MetroCluster executando o ONTAP 9.1 ou posterior

A tabela a seguir mostra o uso da porta ISL para um switch Cisco 9132T.

MetroCluster 1 ou Grupo de RD 1			
Porta	Quatro nós		Oito nós
	9132T (1x LEM)	9132T (2x LEM)	9132T (2x LEM)
ISL1	LEM1-15	LEM2-9	LEM1-13

ISL2	LEM1-16	LEM2-10	LEM1-14
ISL3		LEM2-11	LEM1-15
ISL4		LEM2-12	LEM1-16
ISL5		LEM2-13	
ISL6		LEM2-14	
ISL7		LEM2-15	
ISL8		LEM2-16	

Atribuições de portas para switches FC ao usar sistemas AFF A900

Atribuições de portas para switches FC ao usar sistemas AFF A900 ou FAS9500

Você precisa verificar se está usando as atribuições de portas especificadas quando você faz o cabeamento dos switches FC ao usar o ONTAP 9.10,1 e posterior.

As portas que não são usadas para anexar portas do iniciador, portas FC-VI ou ISLs podem ser reconfiguradas para agir como portas de storage. No entanto, se os RCFs suportados estiverem sendo usados, o zoneamento deve ser alterado em conformidade.

Se os RCFs suportados forem usados, as portas ISL podem não se conetar às mesmas portas mostradas e podem precisar ser reconfiguradas manualmente.

Se você configurou seus switches usando as atribuições de portas do ONTAP 9, poderá continuar a usar as atribuições mais antigas. No entanto, novas configurações que executam o ONTAP 9.1 ou versões posteriores devem usar as atribuições de portas mostradas aqui.

Diretrizes gerais de cabeamento

Você deve estar ciente das seguintes diretrizes ao usar as tabelas de cabeamento:

- Os sistemas de storage AFF A900 ou FAS9500 exigem oito portas FC-VI. Se você estiver usando um AFF A900 ou FAS9500, será necessário usar a configuração de oito portas. Se a configuração incluir outros modelos de sistema de storage, use o cabeamento mostrado nas tabelas, mas ignore o cabeamento para portas FC-VI desnecessárias.
- Se você tiver duas configurações do MetroCluster compartilhando ISLs, use as mesmas atribuições de porta que aquela para um cabeamento MetroCluster de oito nós.
- O número de ISLs que você faz a cabo pode variar dependendo dos requisitos do local.
- Consulte a secção sobre considerações ISL.

  "Considerações para ISLs"

Uso de porta Brocade para controladores AFF A900 ou FAS9500 em uma configuração MetroCluster executando ONTAP 9.10,1 ou posterior

As tabelas a seguir mostram o uso de portas nos switches Brocade. As tabelas mostram a configuração máxima suportada, com oito módulos de controlador em quatro grupos de DR. Os sistemas AFF A900 e FAS9500 têm oito portas FC-VI (a, b, c e d para FC-VI-1 e FC-VI-2)

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)							
MetroCluster 1 ou Grupo de RD 1							
Componente	Porta	Modelo de interrutor Brocade					
		Liga ao FC_switch …	6510	6505, G610	G620, G620-1	G630, G630-1	G720
controller_x_1	Porta a FC-VI-1	1	0	0	0	0	0
	Porta FC-VI-1 b	2	0	0	0	0	0
	Porta FC-VI-1 c	1	1	1	1	1	1
	FC-VI-1 porta d	2	1	1	1	1	1
	Porta a FC-VI-2	1	20	16	16	16	2
	Porta FC-VI-2 b	2	20	16	16	16	2
	Porta FC-VI-2 c	1	21	17	17	17	3
	FC-VI-2 porta d	2	21	17	17	17	3
	HBA porta a	1	2	2	2	2	8
	Porta HBA b	2	2	2	2	2	8
	Porta HBA c	1	3	3	3	3	9
	Porta d. HBA	2	3	3	3	3	9

controller_x_2		Porta a FC-VI-1	1	4	4	4	4	4
		Porta FC-VI-1 b	2	4	4	4	4	4
		Porta FC-VI-1 c	1	5	5	5	5	5
		FC-VI-1 porta d	2	5	5	5	5	5
		Porta a FC-VI-2	1	22	18	20	20	6
		Porta FC-VI-2 b	2	22	18	20	20	6
		Porta FC-VI-2 c	1	23	19	21	21	7
		FC-VI-2 porta d	2	23	19	21	21	7
		HBA porta a	1	6	6	6	6	12
		Porta HBA b	2	6	6	6	6	12
		Porta HBA c	1	7	7	7	7	13
		Porta d. HBA	2	7	7	7	7	13
Pilha 1	bridge_x_1 a	FC1	1	8	8	8	8	10
		FC2	2	8	8	8	8	10
	bridge_x_1 b	FC1	1	9	9	9	9	11
		FC2	2	9	9	9	9	11
Pilha 2	bridge_x_2 a	FC1	1	10	10	10	10	14
		FC2	2	10	10	10	10	14
	bridge_x_2 b	FC1	1	11	11	11	11	15
		FC2	2	11	11	11	11	15
Pilha 3	bridge_x_3 a	FC1	1	12	12	12	12	16
		FC2	2	12	12	12	12	16
	bridge_x_3 b	FC1	1	13	13	13	13	17
		FC2	2	13	13	13	13	17

Empilha y	bridge_x_y a	FC1	1	14	14	14	14	20
		FC2	2	14	14	14	14	20
	ponte_x_y b	FC1	1	15	15	15	15	21
		FC2	2	15	15	15	15	21

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)							
MetroCluster 2 ou Grupo de RD 2							
Componente	Porta	Modelo de interrutor Brocade					
		Liga ao FC_switch …	6510	6505, G610	G620, G620-1	G630, G630-1	G720
controller_x_3	Porta a FC-VI-1	1	24	-	18	18	18
	Porta FC-VI-1 b	2	24	-	18	18	18
	Porta FC-VI-1 c	1	25	-	19	19	19
	FC-VI-1 porta d	2	25	-	19	19	19
	Porta a FC-VI-2	1	36	-	36	36	24
	Porta FC-VI-2 b	2	36	-	36	36	24
	Porta FC-VI-2 c	1	37	-	37	37	25
	FC-VI-2 porta d	2	37	-	37	37	25
	HBA porta a	1	26	-	24	24	26
	Porta HBA b	2	26	-	24	24	26
	Porta HBA c	1	27	-	25	25	27
	Porta d. HBA	2	27	-	25	25	27

controller_x_4		Porta a FC-VI-1	1	28	-	22	22	22
		Porta FC-VI-1 b	2	28	-	22	22	22
		Porta FC-VI-1 c	1	29	-	23	23	23
		FC-VI-1 porta d	2	29	-	23	23	23
		Porta a FC-VI-2	1	38	-	38	38	28
		Porta FC-VI-2 b	2	38	-	38	38	28
		Porta FC-VI-2 c	1	39	-	39	39	29
		FC-VI-2 porta d	2	39	-	39	39	29
		HBA porta a	1	30	-	28	28	30
		Porta HBA b	2	30	-	28	28	30
		Porta HBA c	1	31	-	29	29	31
		Porta d. HBA	2	31	-	29	29	31
Pilha 1	bridge_x_51a	FC1	1	32	-	26	26	32
		FC2	2	32	-	26	26	32
	bridge_x_51b	FC1	1	33	-	27	27	33
		FC2	2	33	-	27	27	33
Pilha 2	bridge_x_52a	FC1	1	34	-	30	30	34
		FC2	2	34	-	30	30	34
	bridge_x_52b	FC1	1	35	-	31	31	35
		FC2	2	35	-	31	31	35
Pilha 3	bridge_x_53a	FC1	1	-	-	32	32	36
		FC2	2	-	-	32	32	36
	bridge_x_53b	FC1	1	-	-	33	33	37
		FC2	2	-	-	33	33	37

Empilha y	bridge_x_5ya	FC1	1	-	-	34	34	38
		FC2	2	-	-	34	34	38
	bridge_x_5yb	FC1	1	-	-	35	35	39
		FC2	2	-	-	35	35	39

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)			
MetroCluster 3 ou Grupo de RD 3			
Componente	Porta	Modelo de interrutor Brocade	
		Liga ao FC_switch…	G630, G630-1
controller_x_5	Porta a FC-VI-1	1	48
	Porta FC-VI-1 b	2	48
	Porta FC-VI-1 c	1	49
	FC-VI-1 porta d	2	49
	Porta a FC-VI-2	1	64
	Porta FC-VI-2 b	2	64
	Porta FC-VI-2 c	1	65
	FC-VI-2 porta d	2	65
	HBA porta a	1	50
	Porta HBA b	2	50
	Porta HBA c	1	51
	Porta d. HBA	2	51
controller_x_6	Porta a FC-VI-1	1	52
	Porta FC-VI-1 b	2	52
	Porta FC-VI-1 c	1	53
	FC-VI-1 porta d	2	53
	Porta a FC-VI-2	1	68
	Porta FC-VI-2 b	2	68
	Porta FC-VI-2 c	1	69
	FC-VI-2 porta d	2	69
	HBA porta a	1	54
	Porta HBA b	2	54
	Porta HBA c	1	55
	Porta d. HBA	2	55

Pilha 1	bridge_x_1a	FC1	1	56
		FC2	2	56
	bridge_x_1b	FC1	1	57
		FC2	2	57
Pilha 2	bridge_x_2a	FC1	1	58
		FC2	2	58
	bridge_x_2b	FC1	1	59
		FC2	2	59
Pilha 3	bridge_x_3a	FC1	1	60
		FC2	2	60
	bridge_x_3b	FC1	1	61
		FC2	2	61
Empilha y	bridge_x_ya	FC1	1	62
		FC2	2	62
	ponte_x_yb	FC1	1	63
		FC2	2	63

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)			
MetroCluster 4 ou Grupo de RD 4			
Componente	Porta	Modelo de interrutor Brocade	
		Liga ao FC_switch…	G630, G630-1
controller_x_7	Porta a FC-VI-1	1	66
	Porta FC-VI-1 b	2	66
	Porta FC-VI-1 c	1	67
	FC-VI-1 porta d	2	67
	Porta a FC-VI-2	1	84
	Porta FC-VI-2 b	2	84
	Porta FC-VI-2 c	1	85
	FC-VI-2 porta d	2	85
	HBA porta a	1	72
	Porta HBA b	2	72
	Porta HBA c	1	73
	Porta d. HBA	2	73

controller_x_8		Porta a FC-VI-1	1	70
		Porta FC-VI-1 b	2	70
		Porta FC-VI-1 c	1	71
		FC-VI-1 porta d	2	71
		Porta a FC-VI-2	1	86
		Porta FC-VI-2 b	2	86
		Porta FC-VI-2 c	1	87
		FC-VI-2 porta d	2	87
		HBA porta a	1	76
		Porta HBA b	2	76
		Porta HBA c	1	77
		Porta d. HBA	2	77
Pilha 1	bridge_x_51a	FC1	1	74
		FC2	2	74
	bridge_x_51b	FC1	1	75
		FC2	2	75
Pilha 2	bridge_x_52a	FC1	1	78
		FC2	2	78
	bridge_x_52b	FC1	1	79
		FC2	2	79
Pilha 3	bridge_x_53a	FC1	1	80
		FC2	2	80
	bridge_x_53b	FC1	1	81
		FC2	2	81
Empilha y	bridge_x_5ya	FC1	1	82
		FC2	2	82
	bridge_x_5yb	FC1	1	83
		FC2	2	83

AFF A900 ou FAS9500 - uso de porta Brocade para ISLs em uma configuração do MetroCluster executando o ONTAP 9.10,1 ou posterior

A tabela a seguir mostra o uso da porta ISL para os switches Brocade em um sistema AFF A900 ou FAS9500.

Os sistemas AFF A900 e FAS9500 suportam oito ISLs. Oito ISLs são suportadas nos switches Brocade 6510, G620, G620-1, G630, G630-1 e G720.

Modelo do interrutor	Porta de ISL	Porta do switch
6510, G620, G620-1, G630, G630-1, G720	ISL1	40
ISL2	41	ISL3
42	ISL4	43
ISL5	44	ISL6
45	ISL7	46
ISL8	47	6505,G610
ISL1	20	
ISL2	21	
ISL3	22	

Uso de porta Cisco para controladores AFF A900 ou FAS9500 em uma configuração MetroCluster executando ONTAP 9.10,1 ou posterior

As tabelas mostram o máximo de configurações suportadas, com oito módulos de controlador AFF A900 ou FAS9500 em um grupo de DR.

- A tabela a seguir mostra sistemas com oito portas FC-VI. O AFF A900 e o FAS9500 têm oito portas FC-VI (a, b, c e d para FC-VI-1 e FC-VI-2).
- O MetroCluster 2 ou DR 2 não é compatível com switches 9132T.

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)				
MetroCluster 1 ou Grupo de RD 1				
Componente	Porta	Modelo de interrutor Cisco		
		Liga ao FC_switch…	9132T (1x LEM)	9132T (2x LEM)

controller_x_1		Porta a FC-VI-1	1	LEM1-1	LEM1-1
		Porta FC-VI-1 b	2	LEM1-1	LEM1-1
		Porta FC-VI-1 c	1	LEM1-2	LEM1-2
		FC-VI-1 porta d	2	LEM1-2	LEM1-2
		Porta a FC-VI-2	1	LEM1-3	LEM1-3
		Porta FC-VI-2 b	2	LEM1-3	LEM1-3
		Porta FC-VI-2 c	1	LEM1-4	LEM1-4
		FC-VI-2 porta d	2	LEM1-4	LEM1-4
		HBA porta a	1	LEM1-5	LEM1-5
		Porta HBA b	2	LEM1-5	LEM1-5
		Porta HBA c	1	LEM1-6	LEM1-6
		Porta d. HBA	2	LEM1-6	LEM1-6
controller_x_2		Porta a FC-VI-1	1	LEM1-7	LEM1-7
		Porta FC-VI-1 b	2	LEM1-7	LEM1-7
		Porta FC-VI-1 c	1	LEM1-8	LEM1-8
		FC-VI-1 porta d	2	LEM1-8	LEM1-8
		Porta a FC-VI-2	1	LEM1-9	LEM1-9
		Porta FC-VI-2 b	2	LEM1-9	LEM1-9
		Porta FC-VI-2 c	1	LEM1-10	LEM1-10
		FC-VI-2 porta d	2	LEM1-10	LEM1-10
		HBA porta a	1	LEM1-11	LEM1-11
		Porta HBA b	2	LEM1-11	LEM1-11
		Porta HBA c	1	LEM1-12	LEM1-12
		Porta d. HBA	2	LEM1-12	LEM1-12
Pilha 1	bridge_x_1a	FC1	1	LEM1-13	LEM1-13
		FC2	2	LEM1-13	LEM1-13
	bridge_x_1b	FC1	1	LEM1-14	LEM1-14
		FC2	2	LEM1-14	LEM1-14
Pilha 2	bridge_x_2a	FC1	1	-	LEM1-15
		FC2	2	-	LEM1-15
	bridge_x_2b	FC1	1	-	LEM1-16
		FC2	2	-	LEM1-16

Pilha 3	bridge_x_3a	FC1	1	-	LEM2-1
		FC2	2	-	LEM2-1
	bridge_x_3b	FC1	1	-	LEM2-2
		FC2	2	-	LEM2-2
Empilha y	bridge_x_ya	FC1	1	-	LEM2-3
		FC2	2	-	LEM2-3
	ponte_x_yb	FC1	1	-	LEM2-4
		FC2	2	-	LEM2-4

- Você pode fazer pontes adicionais para as portas LEM2-5 até LEM2-8 em switches 9132T com 2x módulos LEM.
- Apenas uma (1) pilha de ponte é suportada usando 9132T switches com 1x módulo LEM.

AFF A900 ou FAS9500 - uso de porta Cisco para ISLs em uma configuração de oito nós em uma configuração MetroCluster executando o ONTAP 9.10,1 ou posterior

A tabela a seguir mostra o uso da porta ISL. O uso da porta ISL é o mesmo em todos os switches na configuração.

Modelo do interrutor	Porta de ISL	Porta do switch
Cisco 9132T com 1x LEM	ISL1	LEM1-15
	ISL2	LEM1-16
Cisco 9132T com 2x LEM	ISL1	LEM2-9
	ISL2	LEM2-10
	ISL3	LEM2-11
	ISL4	LEM2-12
	ISL5	LEM2-13
	ISL6	LEM2-14
	ISL7	LEM2-15
	ISL8	LEM2-16

Cabeamento da interconexão de cluster em configurações de oito ou quatro nós

Em configurações de MetroCluster de oito ou quatro nós, você deve fazer o cabeamento da interconexão de cluster entre os módulos de controladora local em cada local.

Sobre esta tarefa

Esta tarefa não é necessária em configurações de MetroCluster de dois nós.

Esta tarefa deve ser executada em ambos os locais do MetroCluster.

Passo

1. Faça a interconexão de cluster de um módulo de controladora para o outro, ou se forem usados switches de interconexão de cluster, de cada módulo de controladora para os switches.

Informações relacionadas

"Documentação dos sistemas de hardware da ONTAP"

"Gerenciamento de rede e LIF"

Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de cluster para que elas tenham conetividade com o cluster no site do parceiro.

Sobre esta tarefa

Esta tarefa deve ser executada em cada módulo do controlador na configuração do MetroCluster.

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

Passo

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

   O peering de cluster pode ser feito em portas dedicadas ou em portas de dados. O uso de portas dedicadas fornece maior taxa de transferência para o tráfego de peering de cluster.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

Cada site do MetroCluster é configurado como um ponto do site do parceiro. Você deve estar familiarizado com os pré-requisitos e diretrizes para configurar os relacionamentos de peering e ao decidir se usar portas compartilhadas ou dedicadas para esses relacionamentos.

"Peering de clusters"

Cabeamento da interconexão de HA

Se você tiver uma configuração de MetroCluster de oito ou quatro nós e os controladores de storage nos pares de HA estiverem em chassi separado, será necessário fazer o cabeamento da interconexão de HA entre as controladoras.

Sobre esta tarefa

- Esta tarefa não se aplica a configurações de MetroCluster de dois nós.
- Esta tarefa deve ser executada em ambos os locais do MetroCluster.
- A interconexão de HA só deve ser cabeada se as controladoras de storage dentro do par de HA estiverem em chassi separado.

  Alguns modelos de controladora de storage oferecem suporte a duas controladoras em um único chassi. Nesse caso, elas usam uma interconexão interna de HA.

Passos

1. Cable a interconexão de HA se o parceiro de HA da controladora de storage estiver em um chassi separado.

   "Documentação dos sistemas de hardware da ONTAP"

2. Se o local do MetroCluster incluir dois pares de HA, repita as etapas anteriores no segundo par de HA.
3. Repita esta tarefa no site do parceiro MetroCluster.

Cabeamento das conexões de dados e gerenciamento

Você deve encaminhar as portas de gerenciamento e dados em cada controlador de storage para as redes do local.

Sobre esta tarefa

Esta tarefa deve ser repetida para cada novo controlador em ambos os locais do MetroCluster.

Você pode conetar as portas de gerenciamento do controlador e do switch de cluster a switches existentes na rede ou a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passo

1. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

   "Documentação dos sistemas de hardware da ONTAP"

Configurar os switches FC

Visão geral da configuração do switch FC

Você pode configurar switches Cisco e Brocade FC usando arquivos RCF ou, se necessário, pode configurar manualmente os switches.

Se você…	Use o procedimento…
Tenha um RCF que atenda aos seus requisitos	• "Configurar switches Brocade FC com arquivos RCF" • "Configurar switches Cisco FC com arquivos RCF"
Não tem um RCF ou um RCF que não atenda aos seus requisitos	• "Configure os switches Brocade FC manualmente" • "Configure os switches Cisco FC manualmente"

Configurar switches Brocade FC com arquivos RCF

Redefinindo o switch Brocade FC para os padrões de fábrica

Antes de instalar uma nova versão de software e arquivos RCF, você deve apagar a

configuração atual do switch e executar a configuração básica.

Sobre esta tarefa

Você deve repetir estas etapas em cada um dos switches FC na configuração da malha do MetroCluster.

Passos

1. Inicie sessão na central como administrador.
2. Desative o recurso Brocade Virtual Fabrics (VF):

   `fosconfig options`

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   WARNING:  This is a disruptive operation that requires a reboot to take
   effect.
   Would you like to continue  [Y/N]: y
   ```

3. Desligue os cabos ISL das portas do interrutor.
4. Desativar o interrutor:

   `switchcfgpersistentdisable`

   ```
   FC_switch_A_1:admin> switchcfgpersistentdisable
   ```

5. Desative a configuração:

   `cfgDisable`

   ```
   FC_switch_A_1:admin> cfgDisable
   You are about to disable zoning configuration. This action will disable
   any previous zoning configuration enabled.
   Do you want to disable zoning configuration? (yes, y, no, n): [no] y
   Updating flash ...
   Effective configuration is empty. "No  Access" default zone mode is ON.
   ```

6. Limpar a configuração:

   `cfgClear`

```
FC_switch_A_1:admin> cfgClear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
Run cfgSave to commit the transaction or cfgTransAbort to
cancel the transaction.
Do you really want to clear all configurations?  (yes, y, no, n): [no] y
```

7. Guardar a configuração:

```
cfgSave
```

```
FC_switch_A_1:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only?  (yes, y, no,
n): [no] y
Updating flash ...
```

8. Defina a configuração padrão:

```
configDefault
```

```
FC_switch_A_1:admin> configDefault
WARNING:  This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

9. Defina a configuração da porta como padrão para todas as portas:

   `portcfgdefault port-number`

   ```
   FC_switch_A_1:admin> portcfgdefault <port number>
   ```

   Você deve concluir esta etapa para cada porta.

10. Verifique se o switch está usando o método POD (Dynamic Port on Demand).

    Para versões do Brocade Fabric os anteriores a 8,0, você executa os seguintes comandos como admin e, para as versões 8,0 e posteriores, os executa como root.

    a. Execute o comando license:

       Para o Fabric os 8,2.x e anteriores

       Executar o comando `licenseport --show`.

       Para o Fabric os 9,0 e posterior

       Executar o comando `license --show -port`.

       ```
       FC_switch_A_1:admin> license --show -port
       24 ports are available in this switch
       Full POD license is installed
       Dynamic POD method is in use
       ```

    b. Ative o usuário raiz se ele estiver desativado pelo Brocade.

       ```
       FC_switch_A_1:admin> userconfig --change root -e yes
       FC_switch_A_1:admin> rootaccess --set consoleonly
       ```

    c. Execute o comando license:

       Para o Fabric os 8,2.x e anteriores

       Executar o comando `licenseport --show`.

       Para o Fabric os 9,0 e posterior

       Executar o comando `license --show -port`.

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Se você estiver executando o Fabric os 8,2.x e anteriores, você deve alterar o método de licença para dinâmico:

```
licenseport --method dynamic
```

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

+

No Fabric os 9,0 e posterior, o método de licença é dinâmico por padrão. O método de licença estática não é suportado.

11. Reinicie o switch:

```
fastBoot
```

```
FC_switch_A_1:admin> fastboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
```

12. Confirme se as configurações padrão foram implementadas:

```
switchShow
```

13. Verifique se o endereço IP está definido corretamente:

```
ipAddrShow
```

Você pode definir o endereço IP com o seguinte comando, se necessário:

```
ipAddrSet
```

Transferir o ficheiro RCF do switch Brocade FC

É necessário fazer o download do arquivo de configuração de referência (RCF) para cada switch na configuração do MetroCluster Fabric.

Sobre esta tarefa

Para usar esses arquivos RCF, o sistema deve estar executando o ONTAP 9.1 ou posterior e você deve usar o layout de porta para o ONTAP 9.1 ou posterior.

Se você estiver planejando usar apenas uma das portas FC nas bridges do FibreBridge, configure manualmente os switches de canal de fibra back-end usando as instruções encontradas na seção ."Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passos

1. Consulte a tabela de arquivos RCF na página de download do Brocade RCF e identifique o arquivo RCF correto para cada switch em sua configuração.

   Os ficheiros RCF têm de ser aplicados aos interrutores corretos.

2. Transfira os ficheiros RCF para os comutadores a partir "Baixar MetroCluster RCF" da página.

   Os arquivos devem ser colocados em um local onde possam ser transferidos para o switch. Há um arquivo separado para cada um dos quatro switches que compõem a malha de dois switches.

3. Repita estas etapas em cada switch na configuração.

Instalar o arquivo RCF do switch Brocade FC

Ao configurar um switch Brocade FC, você pode instalar os arquivos de configuração do switch que fornecem as configurações completas do switch para determinadas configurações.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches Brocade FC na configuração da malha do MetroCluster.
- Se você usar uma configuração xWDM, poderá exigir configurações adicionais nos ISLs. Consulte a documentação do fornecedor xWDM para obter mais informações.

Passos

1. Inicie o processo de download e configuração:

   `configDownload`

   Responda aos prompts como mostrado no exemplo a seguir.

```
FC_switch_A_1:admin> configDownload
Protocol (scp, ftp, sftp, local) [ftp]:
Server Name or IP Address [host]: <user input>
User Name [user]:<user input>
Path/Filename [<home dir>/config.txt]:path to configuration file
Section (all|chassis|switch [all]): all
.
.
.
Do you want to continue [y/n]: y
Password: <user input>
```

Depois de introduzir a sua palavra-passe, o comutador transfere e executa o ficheiro de configuração.

2. Confirme se o arquivo de configuração definiu o domínio do switch:

   `switchShow`

   Cada switch recebe um número de domínio diferente, dependendo do arquivo de configuração usado pelo switch.

   ```
   FC_switch_A_1:admin> switchShow
   switchName: FC_switch_A_1
   switchType: 109.1
   switchState: Online
   switchMode: Native
   switchRole: Subordinate
   switchDomain: 5
   ```

3. Verifique se o switch recebeu o valor de domínio correto, conforme indicado na tabela a seguir.

Malha	Interrutor	Mudar de domínio
1	A_1	5
B_1	7	2
A_2	6	B_2

4. Alterar a velocidade da porta:

   `portcfgspeed`

   ```
   FC_switch_A_1:admin> portcfgspeed port number port speed
   ```

   Por padrão, todas as portas são configuradas para operar a 16 Gbps. Você pode alterar a velocidade da porta pelos seguintes motivos:

   - A velocidade das portas do switch de interconexão deve ser alterada quando um adaptador FC-VI de 8 Gbps é usado e a velocidade da porta do switch deve ser definida como 8 Gbps.
   - A velocidade das portas ISL deve ser alterada quando o ISL não é capaz de funcionar a 16 Gbps.

5. Calcule a distância ISL.

   Devido ao comportamento do FC-VI, você deve definir a distância para 1,5 vezes a distância real com um mínimo de 10 (LE). A distância para o ISL é calculada da seguinte forma, arredondada para o próximo quilômetro completo: 1,5 x distância real.

   Se a distância for de 3 km, então 1,5 x 3 km é de 4,5. Isto é inferior a 10; portanto, você deve definir o ISL para o nível de distância LE.

A distância é de 20 km, depois 1,5 x 20 km 30. Tem de definir o ISL para o nível de distância LS.

6. Defina a distância para cada porta ISL:

   `portcfglongdistance port level vc_link_init -distance distance_value`

   Um valor vc_link_init de 1 usa a palavra "ARB" por padrão. Um valor de 0 usa o fillword "IDLE". O valor necessário pode variar dependendo do link que você usa. Neste exemplo, o padrão é definido e a distância é assumida como 20 km. Portanto, a configuração é "30" com um valor vc_link_init de "1", e a porta ISL é "21".

   Exemplo: LS

   ```
   FC_switch_A_1:admin> portcfglongdistance 21 LS 1 -distance 30
   ```

   Exemplo: LE

   ```
   FC_switch_A_1:admin> portcfglongdistance 21 LE 1
   ```

7. Ativar persistentemente o interrutor:

   `switchcfgpersistentenable`

   O exemplo mostra como ativar persistentemente FC switch_A_1.

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

8. Verifique se o endereço IP está definido corretamente:

   `ipAddrshow`

   ```
   FC_switch_A_1:admin> ipAddrshow
   ```

   Você pode definir o endereço IP, se necessário:

   `ipAddrSet`

9. Defina o fuso horário a partir do prompt de switch:

   `tstimezone --interactive`

   Você deve responder aos prompts conforme necessário.

   ```
   FC_switch_A_1:admin>  tstimezone --interactive
   ```

10. Reinicie o switch:

    `reboot`

    O exemplo mostra como reiniciar o switch FC _A_1.

    ```
    FC_switch_A_1:admin> reboot
    ```

11. Verifique a definição de distância:

    `portbuffershow`

    Um ajuste de distância DE LE aparece como 10 km.

    ```
    FC_Switch_A_1:admin> portbuffershow
    User Port Lx   Max/Resv Buffer Needed  Link     Remaining
    Port Type Mode Buffers  Usage  Buffers Distance Buffers
    ---- ---- ---- ------- ------ ------- --------- ----------
    ...
    21    E    -      8      67     67      30 km
    22    E    -      8      67     67      30 km
    ...
    23    -    8      0       -      -      466
    ```

12. Volte a ligar os cabos ISL às portas dos interrutores onde foram removidos.

    Os cabos ISL foram desligados quando as definições de fábrica foram repostas para as predefinições.

    "Redefinindo o switch Brocade FC para os padrões de fábrica"

13. Validar a configuração.

    a. Verifique se os switches formam uma malha:

       `switchshow`

       O exemplo a seguir mostra a saída para uma configuração que usa ISLs nas portas 20 e 21.

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==========================================
...
20   20  010C00   id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port,
master is Port 20)
...
```

b. Confirme a configuração dos tecidos:

`fabricshow`

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

c. Verifique se os ISLs estão funcionando:

`islshow`

```
FC_switch_A_1:admin> islshow
```

d. Confirme se o zoneamento é replicado corretamente:

`cfgshow` E
`zoneshow`

Ambas as saídas devem mostrar as mesmas informações de configuração e informações de zoneamento para ambos os switches.

e. Se o entroncamento for usado, confirme o entroncamento:

`trunkShow`

```
FC_switch_A_1:admin> trunkshow
```

Configure os switches Cisco FC com arquivos RCF

Redefinindo o switch Cisco FC para os padrões de fábrica

Antes de instalar uma nova versão de software e RCFs, você deve apagar a configuração do switch Cisco e executar a configuração básica.

Sobre esta tarefa

Você deve repetir estas etapas em cada um dos switches FC na configuração da malha do MetroCluster.

As saídas mostradas são para switches IP Cisco; no entanto, estas etapas também são aplicáveis para switches FC Cisco.

Passos

1. Repor as predefinições de fábrica do interrutor:

   a. Apagar a configuração existente
   `write erase`

   b. Volte a carregar o software do switch
   `reload`

   O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt Cancelar provisionamento automático e continuar com a configuração normal?(sim/não)[n], você deve responder **`yes`** para continuar.

   c. No assistente de configuração, introduza as definições básicas do interrutor:
      - Palavra-passe de administrador
      - Mudar nome
      - Configuração de gerenciamento fora da banda
      - Gateway predefinido
      - Serviço SSH (Remote Support Agent).

      Depois de concluir o assistente de configuração, o switch reinicia.

   d. Quando solicitado, introduza o nome de utilizador e a palavra-passe para iniciar sessão no comutador.

   O exemplo a seguir mostra os prompts e as respostas do sistema ao fazer login no switch. Os colchetes de ângulo (**<<<**) mostram onde você insere as informações.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password  **<<<**
  Confirm the password for "admin": password  **<<<**
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

e. Insira informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e insira **`rsa`** a chave SSH como mostrado no exemplo:

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

O conjunto final de prompt completa a configuração:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Guardar a configuração:

```
IP_switch_A_1# copy running-config startup-config
```

3. Reinicie o switch e aguarde até que o switch recarregue:

```
IP_switch_A_1# reload
```

4. Repita as etapas anteriores nos outros três switches na configuração da estrutura do MetroCluster.

É necessário fazer download do arquivo do sistema operacional do switch e do arquivo RCF para cada switch na configuração do MetroCluster Fabric.

Antes de começar

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Sobre esta tarefa

Essas etapas devem ser repetidas em cada um dos switches FC na configuração da malha do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

As saídas mostradas são para switches IP Cisco; no entanto, estas etapas também são aplicáveis para switches FC Cisco.

Passos

1. Transfira o ficheiro de software NX-os suportado.

   "Página de download do Cisco"

2. Copie o software do interrutor para o interrutor:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   Neste exemplo, o `nxos.7.0.3.I4.6.bin` arquivo é copiado do servidor SFTP 10.10.99.99 para o flash de inicialização local:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verifique em cada switch se os arquivos NX-os estão presentes no diretório bootflash de cada switch:

   ```
   dir bootflash
   ```

O exemplo a seguir mostra que os arquivos estão presentes `IP_switch_A_1` no :

```
IP_switch_A_1# dir bootflash:
                   .
                   .
                   .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                   .
                   .
                   .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Instale o software do interrutor:

```
install all system bootflash:nxos.version-number.bin kickstart
bootflash:nxos.version-kickstart-number.bin
```

```
IP_switch_A_1#  install all system bootflash:nxos.7.0.3.I4.6.bin
kickstart bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"system".
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS
...
```

O interrutor reinicia automaticamente após a instalação do software do interrutor.

5. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   Depois que o switch reiniciar, o prompt de login é exibido:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verifique se o software do switch foi instalado:

   `show version`

   O exemplo a seguir mostra a saída:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repita essas etapas nos três switches FC restantes na configuração da malha do MetroCluster.

Download e instalação dos arquivos RCF do Cisco FC

É necessário fazer o download do arquivo RCF para cada switch na configuração do MetroCluster Fabric.

Antes de começar

Esta tarefa requer software de transferência de arquivos, como FTP, Trivial File Transfer Protocol (TFTP), SFTP ou Secure Copy Protocol (SCP), para copiar os arquivos para os switches.

Sobre esta tarefa

Essas etapas devem ser repetidas em cada um dos switches Cisco FC na configuração da malha do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Há quatro arquivos RCF, um para cada um dos quatro switches na configuração da estrutura do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro RCF
FC_switch_A_1	`NX3232_v1.80_Switch-A1.txt`
FC_switch_A_2	`NX3232_v1.80_Switch-A2.txt`
FC_switch_B_1	`NX3232_v1.80_Switch-B1.txt`
FC_switch_B_2	`NX3232_v1.80_Switch-B2.txt`

As saídas mostradas são para switches IP Cisco; no entanto, estas etapas também são aplicáveis para switches FC Cisco.

Passos

1. Transfira os ficheiros RCF do Cisco FC a partir do "Página de download do MetroCluster RCF".
2. Copie os arquivos RCF para os switches.

   a. Copie os arquivos RCF para o primeiro switch:

   ```
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
   bootflash: vrf management
   ```

   Neste exemplo, o `NX3232_v1.80_Switch-A1.txt` arquivo RCF é copiado do servidor SFTP em `10.10.99.99` para o flash de inicialização local. Você deve usar o endereço IP do servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/NX3232_v1.8T-
X1_Switch-A1.txt bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Repita a subetapa anterior para cada uma das outras três centrais, certificando-se de copiar o arquivo RCF correspondente para a central correspondente.

3. Verifique em cada switch se o arquivo RCF está presente no diretório de cada switch `bootflash`:

   `dir bootflash:`

   O exemplo a seguir mostra que os arquivos estão presentes no IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                   .
                   .
                   .
       5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                   .
                   .
                   .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Copie o arquivo RCF correspondente do flash de inicialização local para a configuração em execução em cada switch:

   `copy bootflash:`*`switch-specific-RCF`*`.txt running-config`

5. Copie os arquivos RCF da configuração em execução para a configuração de inicialização em cada switch:

```
copy running-config startup-config
```

Você deve ver saída semelhante ao seguinte:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch_A_1# copy running-config startup-config
```

6. Recarregue o interrutor:

```
reload
```

```
IP_switch_A_1# reload
```

7. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Configuração manual dos switches Brocade FC

Você deve configurar cada uma das malhas de switch Brocade na configuração do MetroCluster.

Antes de começar

- Você deve ter uma estação de trabalho PC ou UNIX com acesso Telnet ou SSH (Secure Shell) aos switches FC.
- Você precisa estar usando quatro switches Brocade compatíveis do mesmo modelo com a mesma versão e licenciamento do sistema operacional (FOS) da Brocade Fabric.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Os quatro switches Brocade compatíveis devem ser conectados a duas malhas de dois switches cada, com cada malha abrangendo ambos os locais.
- Cada controlador de storage deve ter quatro portas do iniciador disponíveis para conexão às malhas do switch. Duas portas de iniciador devem ser conectadas de cada controlador de storage a cada malha.

  Você pode configurar sistemas FAS8020, AFF8020, FAS8200 e AFF A300 com duas portas de iniciadores por controladora (uma única porta de iniciador para cada malha) se todos os critérios a seguir forem atendidos:

  - Há menos de quatro portas do iniciador FC disponíveis para conetar o armazenamento de disco e nenhuma porta adicional pode ser configurada como iniciadores FC.
  - Todos os slots estão em uso e nenhuma placa de iniciador FC pode ser adicionada.

Sobre esta tarefa

- Você deve ativar o entroncamento de enlace Inter-Switch (ISL) quando ele for suportado pelos links.

"Considerações sobre o uso de equipamentos TDM/WDM com configurações MetroCluster conetadas à malha"

- Se você usar uma configuração xWDM, poderá exigir configurações adicionais nos ISLs. Consulte a documentação do fornecedor xWDM para obter mais informações.
- Todos os ISLs devem ter o mesmo comprimento e a mesma velocidade em um tecido.

  Diferentes comprimentos podem ser usados nos diferentes tecidos. A mesma velocidade deve ser usada em todos os tecidos.

- Metro-e e TDM (SONET/SDH) não são suportados, e qualquer enquadramento ou sinalização nativa não FC não é suportado.

  Metro-e significa que o enquadramento ou sinalização Ethernet ocorre nativamente ao longo de uma distância Metro ou através de alguma multiplexação por divisão de tempo (TDM), comutação de etiquetas multiprotocolo (MPLS) ou multiplexação por divisão de comprimento de onda (WDM).

- As extensões TDMs, FCR (roteamento FC nativo) ou FCIP não são compatíveis com a malha de switch MetroCluster FC.
- Certos switches na malha de switch MetroCluster FC são compatíveis com criptografia ou compactação, e às vezes são compatíveis com ambos.

  "Ferramenta de Matriz de interoperabilidade NetApp (IMT)"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- O recurso de malha virtual (VF) do Brocade não é suportado.
- O zoneamento FC baseado na porta de domínio é suportado, mas o zoneamento baseado no nome mundial (WWN) não é suportado.

Revisão dos requisitos de licença do Brocade

Você precisa de certas licenças para os switches em uma configuração do MetroCluster. Você deve instalar essas licenças em todos os quatro switches.

Sobre esta tarefa

A configuração do MetroCluster tem os seguintes requisitos de licença do Brocade:

- Licença de entroncamento para sistemas que utilizam mais de um ISL, conforme recomendado.
- Licença alargada de tecido (para distâncias ISL superiores a 6 km)
- Licença Enterprise para locais com mais de um ISL e uma distância ISL superior a 6 km

  A licença Enterprise inclui o consultor de rede Brocade e todas as licenças, exceto para licenças de porta adicionais.

Passo

1. Verifique se as licenças estão instaladas:

Para o Fabric os 8,2.x e anteriores

Executar o comando `licenseshow`.

Para o Fabric os 9,0 e posterior

Executar o comando `license --show`.

Se você não tiver essas licenças, entre em Contato com seu representante de vendas antes de prosseguir.

Definir os valores do switch Brocade FC para os padrões de fábrica

Você deve definir o switch para seus padrões de fábrica para garantir uma configuração bem-sucedida. Você também deve atribuir a cada switch um nome exclusivo.

Sobre esta tarefa

Nos exemplos deste procedimento, o tecido consiste em BrocadeSwitchA e BrocadeSwitchB.

Passos

1. Faça uma conexão de console e faça login em ambos os switches em uma malha.
2. Desative o interrutor persistentemente:

   `switchcfgpersistentdisable`

   Isso garante que o switch permanecerá desativado após uma reinicialização ou fastboot. Se este comando não estiver disponível, use o `switchdisable` comando.

   O exemplo a seguir mostra o comando no BrocadeSwitchA:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   O exemplo a seguir mostra o comando no BrocadeSwitchB:

   ```
   BrocadeSwitchB:admin> switchcfgpersistentdisable
   ```

3. Defina o nome do interrutor:

   `switchname switch_name`

   Cada um dos switches deve ter um nome exclusivo. Depois de definir o nome, o prompt muda de acordo.

   O exemplo a seguir mostra o comando no BrocadeSwitchA:

   ```
   BrocadeSwitchA:admin> switchname "FC_switch_A_1"
   FC_switch_A_1:admin>
   ```

O exemplo a seguir mostra o comando no BrocadeSwitchB:

```
BrocadeSwitchB:admin> switchname "FC_Switch_B_1"
FC_switch_B_1:admin>
```

4. Defina todas as portas para seus valores padrão:

   `portcfgdefault`

   Isso deve ser feito para todas as portas do switch.

   O exemplo a seguir mostra os comandos em FC_switch_A_1:

```
FC_switch_A_1:admin> portcfgdefault 0
FC_switch_A_1:admin> portcfgdefault 1
...
FC_switch_A_1:admin> portcfgdefault 39
```

   O exemplo a seguir mostra os comandos em FC_switch_B_1:

```
FC_switch_B_1:admin> portcfgdefault 0
FC_switch_B_1:admin> portcfgdefault 1
...
FC_switch_B_1:admin> portcfgdefault 39
```

5. Limpe as informações de zoneamento:

   `cfgdisable`

   `cfgclear`

   `cfgsave`

   O exemplo a seguir mostra os comandos em FC_switch_A_1:

```
FC_switch_A_1:admin> cfgdisable
FC_switch_A_1:admin> cfgclear
FC_switch_A_1:admin> cfgsave
```

   O exemplo a seguir mostra os comandos em FC_switch_B_1:

```
FC_switch_B_1:admin> cfgdisable
FC_switch_B_1:admin> cfgclear
FC_switch_B_1:admin> cfgsave
```

6. Defina as definições gerais do interrutor como predefinição:

   `configdefault`

   O exemplo a seguir mostra o comando em FC_switch_A_1:

   ```
   FC_switch_A_1:admin> configdefault
   ```

   O exemplo a seguir mostra o comando em FC_switch_B_1:

   ```
   FC_switch_B_1:admin> configdefault
   ```

7. Defina todas as portas para o modo não entroncamento:

   `switchcfgtrunk 0`

   O exemplo a seguir mostra o comando em FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgtrunk 0
   ```

   O exemplo a seguir mostra o comando em FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgtrunk 0
   ```

8. Nos switches Brocade 6510, desative o recurso Brocade Virtual Fabrics (VF):

   `fosconfig options`

   O exemplo a seguir mostra o comando em FC_switch_A_1:

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   ```

   O exemplo a seguir mostra o comando em FC_switch_B_1:

   ```
   FC_switch_B_1:admin> fosconfig --disable vf
   ```

9. Limpe a configuração do domínio administrativo (AD):

   O exemplo a seguir mostra os comandos em FC_switch_A_1:

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

O exemplo a seguir mostra os comandos em FC_switch_B_1:

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

10. Reinicie o switch:

    `reboot`

    O exemplo a seguir mostra o comando em FC_switch_A_1:

    ```
    FC_switch_A_1:admin> reboot
    ```

    O exemplo a seguir mostra o comando em FC_switch_B_1:

    ```
    FC_switch_B_1:admin> reboot
    ```

Configurar definições básicas do interrutor

Você deve configurar configurações globais básicas, incluindo o ID do domínio, para switches Brocade.

Sobre esta tarefa

Esta tarefa contém etapas que devem ser executadas em cada switch em ambos os sites do MetroCluster.

Neste procedimento, você define o ID de domínio exclusivo para cada switch, como mostrado no exemplo a seguir. No exemplo, as IDs de domínio 5 e 7 formam Fabric_1 e as IDs de domínio 6 e 8 formam Fabric_2.

- FC_switch_A_1 está atribuído à ID de domínio 5
- FC_switch_A_2 está atribuído à ID de domínio 6
- FC_switch_B_1 está atribuído à ID de domínio 7
- FC_switch_B_2 está atribuído à ID de domínio 8

Passos

1. Entre no modo de configuração:

   `configure`

2. Prossiga através dos prompts:
   a. Defina o ID do domínio para o switch.

b. Pressione **Enter** em resposta aos prompts até chegar ao "ciclo de polling RDP" e, em seguida, defina esse valor para `0` desativar a polling.

c. Pressione **Enter** até retornar ao prompt do switch.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = 5
.
.

RSCN Transmission Mode [yes, y, no, no: [no] y

End-device RSCN Transmission Mode
 (0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric
RSCN): (0..2) [1]
Domain RSCN To End-device for switch IP address or name change
 (0 = disabled, 1 = enabled): (0..1) [0] 1

.
.
RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
```

3. Se você estiver usando dois ou mais ISLs por malha, poderá configurar a entrega em ordem (IOD) de quadros ou a entrega fora de ordem (OOD) de quadros.

> As configurações padrão de IOD são recomendadas. Você deve configurar ODE somente se necessário.

"Considerações sobre o uso de equipamentos TDM/WDM com configurações MetroCluster conetadas à malha"

a. As etapas a seguir devem ser executadas em cada malha de switch para configurar IOD de quadros:

i. Ativar IOD:

```
iodset
```

ii. Defina a política Advanced Performance Tuning (APT) como 1:

```
aptpolicy 1
```

iii. Desativar a partilha de carga dinâmica (DLS):

```
dlsreset
```

iv. Verifique as configurações IOD usando os `iodshow` comandos , `aptpolicy` e `dlsshow` .

Por exemplo, emita os seguintes comandos no FC_switch_A_1:

```
FC_switch_A_1:admin> iodshow
    IOD is set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 1 0(ap)

    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
         0: AP Shared Link Policy
         1: AP Dedicated Link Policy
    command aptpolicy completed

    FC_switch_A_1:admin> dlsshow
    DLS is not set
```

i. Repita estas etapas na segunda tela do interrutor.

b. As etapas a seguir devem ser executadas em cada malha de switch para configurar OID de quadros:

i. Ativar OOD:

```
iodreset
```

ii. Defina a política Advanced Performance Tuning (APT) como 3:

```
aptpolicy 3
```

iii. Desativar a partilha de carga dinâmica (DLS):

```
dlsreset
```

iv. Verifique as configurações do AID:

```
iodshow
```

```
aptpolicy
```

```
dlsshow
```

Por exemplo, emita os seguintes comandos no FC_switch_A_1:

```
FC_switch_A_1:admin> iodshow
    IOD is not set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 3 0(ap)
    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
    command aptpolicy completed


    FC_switch_A_1:admin> dlsshow
    DLS is set by default with current routing policy
```

i. Repita estas etapas na segunda tela do interrutor.

> Ao configurar o ONTAP nos módulos do controlador, O AID deve ser explicitamente configurado em cada módulo do controlador na configuração do MetroCluster.

"Configuração da entrega em ordem ou entrega fora de ordem de quadros no software ONTAP"

4. Verifique se o switch está usando o método de licenciamento de porta dinâmica.

a. Execute o comando license:

Para o Fabric os 8,2.x e anteriores

Executar o comando `licenseport --show`.

Para o Fabric os 9,0 e posterior

Executar o comando `license --show -port`.

```
FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

> As versões do Brocade FabricOS antes de 8,0 executam os seguintes comandos como admin e as versões 8,0 e posteriores os executam como root.

b. Ative o utilizador raiz.

Se o usuário raiz já estiver desativado pelo Brocade, ative o usuário raiz como mostrado no exemplo a

seguir:

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

c. Execute o comando license:

`license --show -port`

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Se você estiver executando o Fabric os 8,2.x e anteriores, você deve alterar o método de licença para dinâmico:

`licenseport --method dynamic`

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

+

> No Fabric os 9,0 e posterior, o método de licença é dinâmico por padrão. O método de licença estática não é suportado.

5. Habilite o trap para MIB T11-FC-ZONE-SERVER para fornecer monitoramento de integridade bem-sucedido dos switches no ONTAP:

a. Ative o MIB-SERVER-T11-FC:

`snmpconfig --set mibCapability -mib_name T11-FC-ZONE-SERVER-MIB -bitmask 0x3f`

b. Ative o trap T11-FC-ZONE-SERVER-MIB:

`snmpconfig --enable mibcapability -mib_name SW-MIB -trap_name swZoneConfigChangeTrap`

c. Repita os passos anteriores no segundo tecido do interrutor.

6. **Opcional**: Se você definir a cadeia de carateres da comunidade para um valor diferente de "público", você deverá configurar os monitores de Saúde do ONTAP usando a cadeia de carateres da comunidade especificada:

a. Altere a cadeia de carateres existente da comunidade:

```
snmpconfig --set snmpv1
```

b. Pressione **Enter** até que você veja o texto "Comunidade (ro): [Público]".

c. Insira a string de comunidade desejada.

Em FC_switch_A_1:

```
FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm     <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]    in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_A_1:admin>
```

Em FC_switch_B_1:

```
FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]     in this example it is set to
"mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_B_1:admin>
```

7. Reinicie o switch:

   `reboot`

   Em FC_switch_A_1:

   ```
   FC_switch_A_1:admin> reboot
   ```

   Em FC_switch_B_1:

   ```
   FC_switch_B_1:admin> reboot
   ```

8. Ativar persistentemente o interrutor:

   `switchcfgpersistentenable`

   Em FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

   Em FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgpersistentenable
   ```

Configurar as definições básicas do interrutor num interrutor Brocade DCX 8510-8

Você deve configurar configurações globais básicas, incluindo o ID do domínio, para switches Brocade.

Sobre esta tarefa

Você deve executar as etapas em cada switch em ambos os sites do MetroCluster. Neste procedimento, você define o ID do domínio para cada switch, conforme mostrado nos exemplos a seguir:

- FC_switch_A_1 está atribuído à ID de domínio 5
- FC_switch_A_2 está atribuído à ID de domínio 6
- FC_switch_B_1 está atribuído à ID de domínio 7
- FC_switch_B_2 está atribuído à ID de domínio 8

No exemplo anterior, as IDs de domínio 5 e 7 formam Fabric_1 e as IDs de domínio 6 e 8 formam Fabric_2.

Você também pode usar este procedimento para configurar os switches quando você estiver usando apenas um switch DCX 8510-8 por site.

Usando este procedimento, você deve criar dois switches lógicos em cada switch Brocade DCX 8510-8. Os dois switches lógicos criados em ambos os switches Brocade DCX8510-8 formarão duas malhas lógicas, como mostrado nos exemplos a seguir:

- ESTRUTURA lógica 1: Switch1/Blade1 e lâmina Switch 2 1
- ESTRUTURA lógica 2: Switch1/Blade2 e lâmina Switch 2 2

Passos

1. Entrar no modo de comando:

   ```
   configure
   ```

2. Prossiga através dos prompts:
   a. Defina o ID do domínio para o switch.
   b. Continue selecionando **Enter** até chegar ao "ciclo de polling RDP" e, em seguida, defina o valor como `0` para desativar a polling.
   c. Selecione **Enter** até retornar ao prompt da central.

   ```
   FC_switch_A_1:admin> configure
   Fabric parameters = y
   Domain_id = `5


   RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
   `
   ```

3. Repita estas etapas em todos os switches em Fabric_1 e Fabric_2.
4. Configure as malhas virtuais.

a. Ative as malhas virtuais no switch:

```
fosconfig --enablevf
```

b. Configure o sistema para usar a mesma configuração base em todos os switches lógicos:

```
configurechassis
```

O exemplo a seguir mostra a saída para o `configurechassis` comando:

```
System (yes, y, no, n): [no] n
cfgload attributes (yes, y, no, n): [no] n
Custom attributes (yes, y, no, n): [no] y
Config Index (0 to ignore): (0..1000) [3]:
```

5. Crie e configure o switch lógico:

```
scfg --create fabricID
```

6. Adicione todas as portas de um blade à malha virtual:

```
lscfg --config fabricID -slot slot -port lowest-port - highest-port
```

> As lâminas que formam uma malha lógica (por exemplo, Switch 1 Blade 1 e Switch 3 Blade 1) precisam ter o mesmo ID de tecido.

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

Informações relacionadas

"Requisitos para usar um switch Brocade DCX 8510-8"

Configuração de e-ports em switches Brocade FC usando portas FC

Para os switches Brocade nos quais os links interswitches (ISL) são configurados usando portas FC, você deve configurar as portas do switch em cada malha de switch que conetam o ISL. Essas portas ISL também são conhecidas como e-ports.

Antes de começar

- Todos os ISLs de uma malha de switch FC devem ser configurados com a mesma velocidade e distância.
- A combinação da porta do switch e do Small Form-factor Pluggable (SFP) deve suportar a velocidade.
- A distância ISL suportada depende do modelo do switch FC.

"Ferramenta de Matriz de interoperabilidade do NetApp"

No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- O link ISL deve ter um lambda dedicado, e o link deve ser suportado pelo Brocade para a distância, tipo de switch e sistema operacional de malha (FOS).

Sobre esta tarefa

Você não deve usar a configuração L0 ao emitir o `portCfgLongDistance` comando. Em vez disso, você deve usar a configuração LE ou LS para configurar a distância nos switches Brocade com um mínimo de nível DE DISTÂNCIA LE.

Você não deve usar a configuração LD ao emitir o `portCfgLongDistance` comando ao trabalhar com o equipamento xWDM/TDM. Em vez disso, você deve usar a configuração LE ou LS para configurar a distância nos switches Brocade.

É necessário executar esta tarefa para cada malha de switch FC.

As tabelas a seguir mostram as portas ISL para diferentes switches e número diferente de ISLs em uma configuração executando o ONTAP 9.1 ou 9,2. Os exemplos mostrados nesta seção são para um switch Brocade 6505. Você deve modificar os exemplos para usar portas que se aplicam ao seu tipo de switch.

Você deve usar o número necessário de ISLs para sua configuração.

Modelo do interrutor	Porta de ISL	Porta do switch
Brocade 6520	Porta ISL 1	23
	Porta ISL 2	47
	Porta ISL 3	71
	Porta ISL 4	95
Brocade 6505	Porta ISL 1	20
	Porta ISL 2	21
	Porta ISL 3	22
	Porta ISL 4	23
Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
	Porta ISL 2	41
	Porta ISL 3	42
	Porta ISL 4	43
	Porta ISL 5	44
	Porta ISL 6	45
	Porta ISL 7	46
	Porta ISL 8	47

Brocade 7810	Porta ISL 1	GE2 Gbps (10 Gbps)
	Porta ISL 2	ge3 Gbps (10 Gbps)
	Porta ISL 3	ge4 Gbps (10 Gbps)
	Porta ISL 4	ge5 Gbps (10 Gbps)
	Porta ISL 5	GE6 Gbps (10 Gbps)
	Porta ISL 6	ge7 Gbps (10 Gbps)
Brocade 7840 **Nota:** o switch Brocade 7840 suporta duas portas VE de 40 Gbps ou até quatro portas VE de 10 Gbps por switch para a criação de ISLs FCIP.	Porta ISL 1	ge0 Gbps (40 Gbps) ou GE2 Gbps (10 Gbps)
	Porta ISL 2	ge1 Gbps (40 Gbps) ou ge3 Gbps (10 Gbps)
	Porta ISL 3	ge10 Gbps (10 Gbps)
	Porta ISL 4	ge11 Gbps (10 Gbps)
Brocade G610	Porta ISL 1	20
	Porta ISL 2	21
	Porta ISL 3	22
	Porta ISL 4	23
Brocade G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
	Porta ISL 2	41
	Porta ISL 3	42
	Porta ISL 4	43
	Porta ISL 5	44
	Porta ISL 6	45
	Porta ISL 7	46

Passos

1. Configure a velocidade da porta:

   `portcfgspeed port-numberspeed`

   Você deve usar a velocidade comum mais alta que é suportada pelos componentes no caminho.

   No exemplo a seguir, existem dois ISLs para cada tecido:

   ```
   FC_switch_A_1:admin> portcfgspeed 20 16
   FC_switch_A_1:admin> portcfgspeed 21 16

   FC_switch_B_1:admin> portcfgspeed 20 16
   FC_switch_B_1:admin> portcfgspeed 21 16
   ```

2. Configure o modo de entroncamento para cada ISL:

   `portcfgtrunkport port-number`

   - Se você estiver configurando os ISLs para entroncamento (IOD), defina o número de porta-numberport do portcfgtrunk como 1 como mostrado no exemplo a seguir:

     ```
     FC_switch_A_1:admin> portcfgtrunkport 20 1
     FC_switch_A_1:admin> portcfgtrunkport 21 1
     FC_switch_B_1:admin> portcfgtrunkport 20 1
     FC_switch_B_1:admin> portcfgtrunkport 21 1
     ```

   - Se você não quiser configurar o ISL para entroncamento (OOD), defina o número portcfgtrunkport como 0 como mostrado no exemplo a seguir:

     ```
     FC_switch_A_1:admin> portcfgtrunkport 20 0
     FC_switch_A_1:admin> portcfgtrunkport 21 0
     FC_switch_B_1:admin> portcfgtrunkport 20 0
     FC_switch_B_1:admin> portcfgtrunkport 21 0
     ```

3. Ative o tráfego de QoS para cada uma das portas ISL:

   `portcfgqos --enable port-number`

   No exemplo a seguir, há dois ISLs por malha de switch:

   ```
   FC_switch_A_1:admin> portcfgqos --enable 20
   FC_switch_A_1:admin> portcfgqos --enable 21

   FC_switch_B_1:admin> portcfgqos --enable 20
   FC_switch_B_1:admin> portcfgqos --enable 21
   ```

4. Verifique as configurações:

   `portCfgShow command`

   O exemplo a seguir mostra a saída para uma configuração que usa dois ISLs cabeados para a porta 20 e a porta 21. A configuração da porta de tronco deve estar LIGADA para IOD e desligada para OOD:

```
Ports of Slot 0   12  13   14 15    16  17  18  19   20  21 22  23    24
25  26  27
----------------+---+---+---+---+-----+---+---+---+----+---+---+---+
-----+---+---+---
Speed             AN  AN  AN  AN    AN  AN  8G  AN   AN  AN  16G  16G
AN  AN  AN  AN
Fill Word         0   0   0   0     0   0   3   0    0   0   3   3     3
0   0   0
AL_PA Offset 13   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Trunk Port        ..  ..  ..  ..    ..  ..  ..  ..   ON  ON  ..  ..
..  ..  ..  ..
Long Distance     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
VC Link Init      ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked L_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked G_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Disabled E_Port   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked E_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
ISL R_RDY Mode    ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
RSCN Suppressed   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Persistent Disable..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
LOS TOV enable    ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
NPIV capability   ON  ON  ON  ON    ON  ON  ON  ON   ON  ON  ON  ON
ON  ON  ON  ON
NPIV PP Limit    126 126 126 126   126 126 126 126  126 126 126 126
126 126 126 126
QOS E_Port        AE  AE  AE  AE    AE  AE  AE  AE   AE  AE  AE  AE
AE  AE  AE  AE
Mirror Port       ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
```

```
Rate Limit         ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Credit Recovery   ON  ON  ON  ON    ON  ON  ON  ON   ON  ON  ON  ON
ON  ON  ON  ON
Fport Buffers      ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Port Auto Disable ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
CSCTL mode         ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..

Fault Delay       0  0  0  0    0  0  0  0   0  0  0  0    0  0  0  0
```

5. Calcule a distância ISL.

   Devido ao comportamento do FC-VI, a distância deve ser definida para 1,5 vezes a distância real com uma distância mínima de 10 km (usando o nível de distância LE).

   A distância para o ISL é calculada da seguinte forma, arredondada para o próximo quilômetro completo:

   1,5 x real_distance: distância

   Se a distância for de 3 4,5 km, então 1,5 x 3 km é inferior a 10 km, portanto, o ISL deve ser definido para o nível de distância LE.

   Se a distância for de 20 km, então 1,5 x 20 km é de 30 km. O ISL deve ser definido para 30 km e deve usar o nível de distância LS.

6. Defina a distância em cada porta ISL:

   `portcfglongdistance` *`portdistance-level`* `vc_link_init` *`distance`*

   Um `vc_link_init` valor de `1` usa a palavra de preenchimento ARB (padrão). Um valor de `0` usos OCIOSOS. O valor necessário pode depender do link que está sendo usado. Os comandos devem ser repetidos para cada porta ISL.

   Para uma distância ISL de 3 km, conforme indicado no exemplo no passo anterior, a definição é de 4,5 km com o valor predefinido `vc_link_init` de `1`. Uma vez que uma definição de 4,5 km é inferior a 10 km, o porto tem de ser definido para o nível DE distância LE:

   ```
   FC_switch_A_1:admin> portcfglongdistance 20 LE 1

   FC_switch_B_1:admin> portcfglongdistance 20 LE 1
   ```

   Para uma distância ISL de 20 km, como indicado no exemplo no passo anterior, a definição é de 30 km com o valor vc_link_init predefinido de `1`:

```
FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30

FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30
```

7. Verifique a definição de distância:

   `portbuffershow`

   Um nível DE distância DE LE aparece como 10 km.

   O exemplo a seguir mostra a saída para uma configuração que usa ISLs na porta 20 e na porta 21:

```
FC_switch_A_1:admin> portbuffershow

User  Port     Lx      Max/Resv    Buffer Needed    Link      Remaining
Port  Type    Mode     Buffers     Usage  Buffers   Distance  Buffers
----  ----    ----     -------     ------ -------   --------- ---------
...
 20     E      -          8         67      67       30km
 21     E      -          8         67      67       30km
...
 23            -          8          0      -        -        466
```

8. Verifique se ambos os switches formam uma única malha:

   `switchshow`

   O exemplo a seguir mostra a saída para uma configuração que usa ISLs na porta 20 e na porta 21:

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==========================================
...
20   20  010C00   id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port, master
is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       7
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State Proto
==========================================
...
20   20  030C00   id    16G  Online  FC  LE E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)(Trunk master)
21   21  030D00   id    16G  Online  FC  LE E-Port  (Trunk port, master
is Port 20)
...
```

9. Confirme a configuração dos tecidos:

```
fabricshow
```

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

```
FC_switch_B_1:admin> fabricshow
   Switch ID   Worldwide Name     Enet IP Addr FC IP Addr   Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"

3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1
```

10. Confirme o entroncamento dos ISLs:

`trunkshow`

- Se você estiver configurando os ISLs para entroncamento (IOD), verá uma saída semelhante à seguinte:

```
FC_switch_A_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
 FC_switch_B_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16
```

- Se você não estiver configurando os ISLs para entroncamento (OOD), você verá uma saída semelhante à seguinte:

```
FC_switch_A_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
 2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER
FC_switch_B_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
 2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER
```

11. Repita Passo 1 a Passo 10 para a segunda malha de switch FC.

Informações relacionadas

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Configurando portas VE de 10 Gbps em switches Brocade FC 7840

Ao usar as portas VE de 10 Gbps (que usam FCIP) para ISLs, você deve criar interfaces IP em cada porta e configurar túneis e circuitos FCIP em cada túnel.

Sobre esta tarefa

Esse procedimento deve ser executado em cada malha de switch na configuração do MetroCluster.

Os exemplos deste procedimento pressupõem que os dois switches Brocade 7840 têm os seguintes endereços IP:

- FC_switch_A_1 é local.
- FC_switch_B_1 é remoto.

Passos

1. Crie endereços de interface IP (ipif) para as portas de 10 Gbps em ambos os switches na malha:

   ```
   portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_IP_address
   netmask netmask_number vlan 2 mtu auto
   ```

   O comando a seguir cria endereços ipif nas portas GE2.DP0 e ge3.DP0 de FC_switch_A_1:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   O comando a seguir cria endereços ipif nas portas GE2.DP0 e ge3.DP0 de FC_switch_B_1:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

2. Verifique se os endereços ipif foram criados com sucesso em ambos os switches:

   ```
   portshow ipif all
   ```

   O comando a seguir mostra os endereços ipif no switch FC_switch_A_1:

```
FC_switch_A_1:root> portshow ipif all

 Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.71                     / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.71                     / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

O comando a seguir mostra os endereços ipif no switch FC_switch_B_1:

```
FC_switch_B_1:root> portshow ipif all

 Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.72                     / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.72                     / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. Crie o primeiro dos dois túneis FCIP usando as portas no DP0:

   `portcfg fciptunnel`

   Este comando cria um túnel com um único circuito.

   O comando a seguir cria o túnel no switch FC_switch_A_1:

```
portcfg fciptunnel 24 create -S 10.10.20.71  -D 10.10.20.72 -b 10000000
-B 10000000
```

   O comando a seguir cria o túnel no switch FC_switch_B_1:

```
portcfg fciptunnel 24 create -S 10.10.20.72  -D 10.10.20.71 -b 10000000
-B 10000000
```

4. Verifique se os túneis FCIP foram criados com sucesso:

   `portshow fciptunnel all`

   O exemplo a seguir mostra que os túneis foram criados e os circuitos estão ativos:

```
FC_switch_B_1:root>

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
-------------------------------------------------------------------------
--------
 24    -         Up      ---------     2d8m    0.05    0.41   3      -
-
-------------------------------------------------------------------------
--------
 Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                 a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                 I=IP-Ext
```

5. Criar um circuito adicional para DP0.

   O seguinte comando cria um circuito no interrutor FC_switch_A_1 para DP0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72  --min
-comm-rate 5000000 --max-comm-rate 5000000
```

   O seguinte comando cria um circuito no interrutor FC_switch_B_1 para DP0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71  --min
-comm-rate 5000000 --max-comm-rate 5000000
```

6. Verifique se todos os circuitos foram criados com sucesso:

   `portshow fcipcircuit all`

   O seguinte comando mostra os circuitos e o respetivo estado:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
-------------------------------------------------------------------------
--------
 24    0 ge2     Up      ---va---4    2d12m    0.02    0.03   3
10000/10000 0/-
 24    1 ge3     Up      ---va---4    2d12m    0.02    0.04   3
10000/10000 0/-
-------------------------------------------------------------------------
--------
 Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                 ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
```

Configuração de portas VE de 40 Gbps em switches FC Brocade 7810 e 7840

Ao usar as duas portas VE de 40 GbE (que usam FCIP) para ISLs, você deve criar interfaces IP em cada porta e configurar túneis e circuitos FCIP em cada túnel.

Sobre esta tarefa

Esse procedimento deve ser executado em cada malha de switch na configuração do MetroCluster.

Os exemplos deste procedimento utilizam dois interrutores:

- FC_switch_A_1 é local.
- FC_switch_B_1 é remoto.

Passos

1. Crie endereços de interface IP (ipif) para as portas de 40 Gbps em ambos os switches na malha:

   `portcfg ipif FC_switch_namefirst_port_name create FC_switch_IP_address netmask netmask_number vlan 2 mtu auto`

   O comando a seguir cria endereços ipif nas portas ge0.DP0 e ge1.DP0 de FC_switch_A_1:

   ```
   portcfg ipif  ge0.dp0 create  10.10.82.10 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge1.dp0 create  10.10.82.11 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   O comando a seguir cria endereços ipif nas portas ge0.DP0 e ge1.DP0 de FC_switch_B_1:

```
portcfg ipif  ge0.dp0 create  10.10.83.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif  ge1.dp0 create  10.10.83.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. Verifique se os endereços ipif foram criados com sucesso em ambos os switches:

   `portshow ipif all`

   O exemplo a seguir mostra as interfaces IP em FC_switch_A_1:

```
Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
---
-----
 ge0.dp0      10.10.82.10                      / 16   AUTO  2     U R M
 ge1.dp0      10.10.82.11                      / 16   AUTO  2     U R M
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

   O exemplo a seguir mostra as interfaces IP em FC_switch_B_1:

```
Port         IP Address                      / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge0.dp0      10.10.83.10                      / 16   AUTO  2     U R M
 ge1.dp0      10.10.83.11                      / 16   AUTO  2     U R M
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. Crie o túnel FCIP em ambos os switches:

   `portcfig fciptunnel`

   O seguinte comando cria o túnel em FC_switch_A_1:

```
portcfg fciptunnel 24 create -S 10.10.82.10  -D 10.10.83.10 -b 10000000
-B 10000000
```

O seguinte comando cria o túnel em FC_switch_B_1:

```
portcfg fciptunnel 24 create -S 10.10.83.10  -D 10.10.82.10 -b 10000000
-B 10000000
```

4. Verifique se o túnel FCIP foi criado com sucesso:

   `portshow fciptunnel all`

   O exemplo a seguir mostra que o túnel foi criado e os circuitos estão ativos:

```
FC_switch_A_1:root>

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
--------------------------------------------------------------------------
--------
 24    -         Up      ---------     2d8m    0.05    0.41   3      -
-
 --------------------------------------------------------------------------
---------
 Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                 a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                 I=IP-Ext
```

5. Crie um circuito adicional em cada interrutor:

   `portcfg fcipcircuit 24 create 1 -S source-IP-address -D destination-IP-address --min-comm-rate 10000000 --max-comm-rate 10000000`

   O seguinte comando cria um circuito no interrutor FC_switch_A_1 para DP0:

```
portcfg fcipcircuit 24  create 1 -S 10.10.82.11 -D 10.10.83.11  --min
-comm-rate 10000000 --max-comm-rate 10000000
```

   O seguinte comando cria um circuito no interrutor FC_switch_B_1 para dp1:

```
portcfg fcipcircuit 24 create 1  -S 10.10.83.11 -D 10.10.82.11  --min
-comm-rate 10000000 --max-comm-rate 10000000
```

6. Verifique se todos os circuitos foram criados com sucesso:

   `portshow fcipcircuit all`

   O exemplo a seguir lista os circuitos e mostra que seu OpStatus está ativado:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
--------------------------------------------------------------------
--------
 24    0 ge0     Up      ---va---4    2d12m    0.02    0.03   3
10000/10000 0/-
 24    1 ge1     Up      ---va---4    2d12m    0.02    0.04   3
10000/10000 0/-
 ------------------------------------------------------------------
---------
 Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                 ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
```

Configurando as portas não-e no switch Brocade

Você deve configurar as portas não-e no switch FC. Em uma configuração MetroCluster, essas são as portas que conetam o switch aos iniciadores HBA, interconexões FC-VI e pontes FC-para-SAS. Estas etapas devem ser feitas para cada porta.

Sobre esta tarefa

No exemplo a seguir, as portas conetam uma ponte FC-para-SAS:

- Porta 6 no FC_FC_switch_A_1 no local_A
- Porta 6 no FC_FC_switch_B_1 no local_B

Passos

1. Configure a velocidade da porta para cada porta não-e:

   `portcfgspeed portspeed`

   Você deve usar a velocidade comum mais alta, que é a velocidade mais alta suportada por todos os componentes no caminho de dados: O SFP, a porta do switch na qual o SFP está instalado e o dispositivo conetado (HBA, bridge, etc.).

   Por exemplo, os componentes podem ter as seguintes velocidades suportadas:

- O SFP é capaz de 4, 8 ou 16 GB.
- A porta do switch é capaz de 4, 8 ou 16 GB.
- A velocidade máxima do HBA ligado é de 16 GB. A velocidade comum mais alta neste caso é de 16 GB, portanto, a porta deve ser configurada para uma velocidade de 16 GB.

```
FC_switch_A_1:admin> portcfgspeed 6 16

FC_switch_B_1:admin> portcfgspeed 6 16
```

2. Verifique as configurações:

   `portcfgshow`

```
FC_switch_A_1:admin> portcfgshow

FC_switch_B_1:admin> portcfgshow
```

   Na saída de exemplo, a porta 6 tem as seguintes configurações; a velocidade é definida como 16G:

```
Ports of Slot 0                    0   1   2   3   4   5   6   7   8
-----------------------------------+---+---+---+--+---+---+---+---+--
Speed                              16G 16G 16G 16G 16G 16G 16G 16G 16G
AL_PA Offset 13                    ..  ..  ..  ..  ..  ..  ..  ..  ..
Trunk Port                         ..  ..  ..  ..  ..  ..  ..  ..  ..
Long Distance                      ..  ..  ..  ..  ..  ..  ..  ..  ..
VC Link Init                       ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked L_Port                      -   -   -   -   -  -   -   -   -
Locked G_Port                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Disabled E_Port                    ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked E_Port                      ..  ..  ..  ..  ..  ..  ..  ..  ..
ISL R_RDY Mode                     ..  ..  ..  ..  ..  ..  ..  .. ..
RSCN Suppressed                    ..  ..  ..  ..  ..  ..  ..  .. ..
Persistent Disable                 ..  ..  ..  ..  ..  ..  ..  .. ..
LOS TOV enable                     ..  ..  ..  ..  ..  ..  ..  .. ..
NPIV capability                    ON  ON  ON  ON  ON  ON  ON  ON  ON
NPIV PP Limit                      126 126 126 126 126 126 126 126 126
QOS Port                           AE  AE  AE  AE  AE  AE  AE  AE  ON
EX Port                            ..  ..  ..  ..  ..  ..  ..  ..  ..
Mirror Port                        ..  ..  ..  ..  ..  ..  ..  ..  ..
Rate Limit                         ..  ..  ..  ..  ..  ..  ..  ..  ..
Credit Recovery                    ON  ON  ON  ON  ON  ON  ON  ON  ON
Fport Buffers                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Eport Credits                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Port Auto Disable                  ..  ..  ..  ..  ..  ..  ..  ..  ..
CSCTL mode                         ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port mode                        ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port over DWDM                   ..  ..  ..  ..  ..  ..  ..  ..  ..
FEC                                ON  ON  ON  ON  ON  ON  ON  ON  ON
Fault Delay                        0   0   0   0   0   0   0   0   0
Non-DFE                            ..  ..  ..  ..  ..  ..  ..  ..  ..
```

Configurando a compressão em portas ISL em um switch Brocade G620

Se você estiver usando switches Brocade G620 e habilitando a compactação nos ISLs, você deverá configurá-lo em cada e-port nos switches.

Sobre esta tarefa

Esta tarefa tem de ser executada nas portas ISL em ambos os interrutores utilizando o ISL.

Passos

1. Desative a porta na qual você deseja configurar a compactação:

   ```
   portdisable port-id
   ```

2. Ativar a compressão na porta:

```
portCfgCompress --enable port-id
```

3. Ative a porta para ativar a configuração com compactação:

```
portenable port-id
```

4. Confirme se a definição foi alterada:

```
portcfgshow port-id
```

O exemplo a seguir habilita a compactação na porta 0.

```
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

Você pode usar o comando islShow para verificar se o e_port está on-line com criptografia ou compactação configurada e ativa.

```
FC_switch_A_1:admin> islshow
  1: 0-> 0 10:00:c4:f5:7c:8b:29:86   5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

Você pode usar o comando portEncCompShow para ver quais portas estão ativas. Neste exemplo, você pode ver que a criptografia e a compactação estão configuradas e ativas na porta 0.

```
FC_switch_A_1:admin> portenccompshow
User      Encryption                  Compression           Config
Port   Configured    Active   Configured   Active  Speed
----   ----------    -------  ----------   ------  -----
  0    Yes            Yes        Yes             Yes        16G
```

Configuração de zoneamento em switches Brocade FC

É necessário atribuir as portas do switch a zonas separadas para separar o tráfego de armazenamento e controlador.

Zoneamento para portas FC-VI

Para cada grupo de DR no MetroCluster, é necessário configurar duas zonas para as conexões FC-VI que permitem tráfego de controlador para controlador. Essas zonas contêm as portas do switch FC que se conetam às portas FC-VI do módulo do controlador. Essas zonas são zonas de qualidade de Serviço (QoS).

Um nome de zona QoS começa com o prefixo QOSHid_, seguido por uma cadeia de carateres definida pelo usuário para diferenciá-la de uma zona regular. Essas zonas de QoS são as mesmas, independentemente do modelo de ponte FibreBridge que está sendo usado.

Cada zona contém todas as portas FC-VI, uma para cada cabo FC-VI de cada controlador. Essas zonas são configuradas para alta prioridade.

As tabelas a seguir mostram as zonas FC-VI para dois grupos de DR.

Grupo DR 1 : zona FC-VI QOSH1 para porta FC-VI a / c

Switch FC	Local	Mudar de domínio	porta 6505 / 6510	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	0	0	0	Controller_A_1 porta FC-VI a
FC_switch_A_1	A	5	1	1	1	Controlador_A_1 porta FC-VI c
FC_switch_A_1	A	5	4	4	4	Controller_A_2 porta FC-VI a
FC_switch_A_1	A	5	5	5	5	Controlador_A_2 porta FC-VI c
FC_switch_B_1	B	7	0	0	0	Controlador_B_1 porta FC-VI a
FC_switch_B_1	B	7	1	1	1	Controlador_B_1 porta FC-VI c
FC_switch_B_1	B	7	4	4	4	Controlador_B_2 porta FC-VI a
FC_switch_B_1	B	7	5	5	5	Controlador_B_2 porta FC-VI c

Zona em tecido_1	Portos membros
QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5

Grupo DR 1 : zona FC-VI QOSH1 para porta FC-VI b / d

Switch FC	Local	Mudar de domínio	porta 6505 / 6510	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	0	0	0	Controlador_A_1 porta FC-VI b
			1	1	1	Controller_A_1 porta FC-VI d
			4	4	4	Controlador_A_2 porta FC-VI b
			5	5	5	Controller_A_2 porta FC-VI d
FC_switch_B_2	B	8	0	0	0	Controlador_B_1 porta FC-VI b
			1	1	1	Controlador_B_1 porta FC-VI d
			4	4	4	Controlador_B_2 porta FC-VI b
			5	5	5	Controlador_B_2 porta FC-VI d

Zona em tecido_1	Portos membros
QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5

Grupo DR 2 : zona FC-VI QOSH2 para porta FC-VI a / c

Switch FC	Local	Mudar de domínio	Porta do switch			Liga a…
			6510	6520	G620	
FC_switch_A_1	A	5	24	48	18	Controller_A_3 porta FC-VI a
			25	49	19	Controlador_A_3 porta FC-VI c
			28	52	22	Controller_A_4 porta FC-VI a

Switch FC	Local	Mudar de domínio	Porta do switch			Liga a…
			29	53	23	Controlador_A_4 porta FC-VI c
FC_switch_B_1	B	7	24	48	18	Controlador_B_3 porta FC-VI a
			25	49	19	Controlador_B_3 porta FC-VI c
			28	52	22	Controlador_B_4 porta FC-VI a
			29	53	23	Controlador_B_4 porta FC-VI c

Zona em tecido_1	Portos membros
QOSH2_MC2_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
QOSH2_MC2_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

Grupo DR 2 : zona FC-VI QOSH2 para porta FC-VI b / d

Switch FC	Local	Mudar de domínio	porta 6510	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	24	48	18	Controlador_A_3 porta FC-VI b
FC_switch_A_2	A	6	25	49	19	Controller_A_3 porta FC-VI d
FC_switch_A_2	A	6	28	52	22	Controlador_A_4 porta FC-VI b
FC_switch_A_2	A	6	29	53	23	Controller_A_4 porta FC-VI d
FC_switch_B_2	B	8	24	48	18	Controlador_B_3 porta FC-VI b
FC_switch_B_2	B	8	25	49	19	Controlador_B_3 porta FC-VI d

Switch FC	Local	Mudar de domínio	porta 6510	porta 6520	Porta G620	Liga a…
FC_switch_B_2	B	8	28	52	22	Controlador_B_4 porta FC-VI b
FC_switch_B_2	B	8	29	53	23	Controlador_B_4 porta FC-VI d

Zona em tecido_2	Portos membros
QOSH2_MC2_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
QOSH2_MC2_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

A tabela a seguir mostra um resumo das zonas FC-VI:

Malha	Nome da zona	Portos membros
FC_switch_A_1 e FC_switch_B_1	QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
	QOSH2_MC1_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28; 7,29
	QOSH2_MC1_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52; 7,53
FC_switch_A_2 e FC_switch_B_2	QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
	QOSH2_MC1_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28; 8,29
	QOSH2_MC1_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52; 8,53

Zoneamento para pontes FibreBridge 7500N ou 7600N usando uma porta FC

Se você estiver usando bridges do FibreBridge 7500N ou 7600N usando apenas uma das duas portas FC, será necessário criar zonas de armazenamento para as portas de ponte. Você deve entender as zonas e as portas associadas antes de configurar as zonas.

Os exemplos mostram zoneamento apenas para o grupo DR 1. Se sua configuração incluir um segundo grupo de DR, configure o zoneamento para o segundo grupo de DR da mesma maneira, usando as portas correspondentes dos controladores e bridges.

Zonas necessárias

É necessário configurar uma zona para cada uma das portas FC de ponte FC para SAS que permita tráfego entre iniciadores em cada módulo de controladora e essa ponte FC para SAS.

Cada zona de armazenamento contém nove portas:

- Oito portas do iniciador HBA (duas conexões para cada controlador)
- Uma porta que se conecta a uma porta FC em ponte FC FC de FC para SAS

As zonas de armazenamento usam zoneamento padrão.

Os exemplos mostram dois pares de pontes conetando dois grupos de pilha em cada local. Como cada ponte usa uma porta FC, há um total de quatro zonas de storage por malha (oito no total).

Nomenclatura da ponte

As bridges usam o seguinte exemplo de nomeação: bridge_site_stack grouplocation em par

Esta parte do nome…	Identifica o…	Valores possíveis…
local	Local no qual o par de pontes reside fisicamente.	A ou B
grupo de pilha	Número do grupo de pilha ao qual o par de ponte se coneta. FibreBridge 7600N ou 7500N bridges suportam até quatro stacks no grupo stack. O grupo de stack não pode conter mais de 10 gavetas de storage.	1, 2, etc.
localização em par	Ponte dentro do par de ponte.Um par de pontes se coneta a um grupo de pilha específico.	a ou b

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Grupo DR 1 - pilha 1 no local_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

Switch FC	**Local**	**Mudar de domínio**	**Porta do switch Brocade 6505, 6510, 6520, G620 ou G610**	**Liga a…**
FC_switch_A_1	A	5	2	Controlador_A_1 porta 0a

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	5	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	7	Controlador_A_2 porta 0C
FC_switch_A_1	A	5	8	bridge_A_1a FC1
FC_switch_B_1	B	7	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	6	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	7	Controlador_B_2 porta 0C

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	6	2	Controlador_A_1 porta 0b
FC_switch_A_1	A	6	3	Controlador_A_1 porta 0d
FC_switch_A_1	A	6	6	Controlador_A_2 porta 0b
FC_switch_A_1	A	6	7	Controlador_A_2 porta 0d
FC_switch_A_1	A	6	8	bridge_A_1b FC1
FC_switch_B_1	B	8	2	Controlador_B_1 porta 0b
FC_switch_B_1	B	8	3	Controlador_B_1 porta 0d

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_B_1	B	8	6	Controlador_B_2 porta 0b
FC_switch_B_1	B	8	7	Controlador_B_2 porta 0d

Zona em tecido_2	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8

Grupo DR 1 - pilha 2 no local_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	5	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	7	Controlador_A_2 porta 0C
FC_switch_A_1	A	5	9	bridge_A_2a FC1
FC_switch_B_1	B	7	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	6	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	7	Controlador_B_2 porta 0C

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1:

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	6	2	Controlador_A_1 porta 0b
FC_switch_A_1	A	6	3	Controlador_A_1 porta 0d
FC_switch_A_1	A	6	6	Controlador_A_2 porta 0b
FC_switch_A_1	A	6	7	Controlador_A_2 porta 0d
FC_switch_A_1	A	6	9	bridge_A_2b FC1
FC_switch_B_1	B	8	2	Controlador_B_1 porta 0b
FC_switch_B_1	B	8	3	Controlador_B_1 porta 0d
FC_switch_B_1	B	8	6	Controlador_B_2 porta 0b
FC_switch_B_1	B	8	7	Controlador_B_2 porta 0d

Zona em tecido_2	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9

Grupo DR 1 - pilha 1 no local_B

MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

Switch FC	Local	Mudar de domínio	Interrutor Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	5	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	7	Controlador_A_2 porta 0C
FC_switch_B_1	B	7	2	Controlador_B_1 porta 0a

Switch FC	Local	Mudar de domínio	Interrutor Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_B_1	B	7	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	6	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	7	Controlador_B_2 porta 0C
FC_switch_B_1	B	7	8	bridge_B_1a FC1

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1:

Switch FC	Local	Mudar de domínio	Interrutor Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	6	2	Controlador_A_1 porta 0b
FC_switch_A_1	A	6	3	Controlador_A_1 porta 0d
FC_switch_A_1	A	6	6	Controlador_A_2 porta 0b
FC_switch_A_1	A	6	7	Controlador_A_2 porta 0d
FC_switch_B_1	B	8	2	Controlador_B_1 porta 0b
FC_switch_B_1	B	8	3	Controlador_B_1 porta 0d
FC_switch_B_1	B	8	6	Controlador_B_2 porta 0b
FC_switch_B_1	B	8	7	Controlador_B_2 porta 0d
FC_switch_B_1	B	8	8	bridge_B_1b FC1

Zona em tecido_2	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8

Grupo DR 1 - pilha 2 no local_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	5	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	7	Controlador_A_2 porta 0C
FC_switch_B_1	B	7	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	6	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	7	Controlador_B_2 porta 0C
FC_switch_B_1	B	7	9	bridge_b_2a FC1

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_b_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1:

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_A_1	A	6	2	Controlador_A_1 porta 0b
FC_switch_A_1	A	6	3	Controlador_A_1 porta 0d
FC_switch_A_1	A	6	6	Controlador_A_2 porta 0b
FC_switch_A_1	A	6	7	Controlador_A_2 porta 0d
FC_switch_B_1	B	8	2	Controlador_B_1 porta 0b
FC_switch_B_1	B	8	3	Controlador_B_1 porta 0d

Switch FC	Local	Mudar de domínio	Porta do switch Brocade 6505, 6510, 6520, G620 ou G610	Liga a…
FC_switch_B_1	B	8	6	Controlador_B_2 porta 0b
FC_switch_B_1	B	8	7	Controlador_B_2 porta 0d
FC_switch_B_1	B	8	9	bridge_B_1b FC1

Zona em tecido_2	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Resumo das zonas de armazenamento

Malha	Nome da zona	Portos membros
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Zoneamento para pontes FibreBridge 7500N usando ambas as portas FC

Se você estiver usando bridges do FibreBridge 7500N com ambas as portas FC, será necessário criar zonas de armazenamento para as portas de ponte. Você deve entender as zonas e as portas associadas antes de configurar as zonas.

Zonas necessárias

É necessário configurar uma zona para cada uma das portas FC de ponte FC para SAS que permita tráfego entre iniciadores em cada módulo de controladora e essa ponte FC para SAS.

Cada zona de armazenamento contém cinco portas:

- Quatro portas do iniciador HBA (uma conexão para cada controlador)
- Uma porta que se conecta a uma porta FC em ponte FC FC de FC para SAS

As zonas de armazenamento usam zoneamento padrão.

Os exemplos mostram dois pares de pontes conetando dois grupos de pilha em cada local. Como cada ponte usa uma porta FC, há um total de oito zonas de storage por malha (dezesseis no total).

Nomenclatura da ponte

As bridges usam o seguinte exemplo de nomeação: bridge_site_stack grouplocation em par

Esta parte do nome…	Identifica o…	Valores possíveis…
local	Local no qual o par de pontes reside fisicamente.	A ou B
grupo de pilha	Número do grupo de pilha ao qual o par de ponte se coneta. FibreBridge 7600N ou 7500N bridges suportam até quatro stacks no grupo stack. O grupo de stack não pode conter mais de 10 gavetas de storage.	1, 2, etc.
localização em par	Ponte dentro do par de pontes. Um par de bridges se coneta a um grupo de pilha específico.	a ou b

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Grupo DR 1 - pilha 1 no local_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

Switch FC	Local	Mudar de domínio	6505 / 6510 / G610 / G620 porta	porta 6520	Liga a…
FC_switch_A_1	A	5	2	2	Controlador_A_1 porta 0a

FC_switch_A_1	A	5	6	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	8	8	bridge_A_1a FC1
FC_switch_B_1	B	7	2	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	6	6	Controlador_B_2 porta 0a

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	3	3	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	7	7	7	Controlador_A_2 porta 0C
FC_switch_A_1	A	5	9	9	9	bridge_A_1b FC1
FC_switch_B_1	B	7	3	3	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	7	7	7	Controlador_B_2 porta 0C

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

Switch FC	Local	Mudar de domínio	6505 / 6510 / G610	6520	G620	Liga a…
FC_switch_A_2	A	6	2	2	2	Controlador_A_1 porta 0b

FC_switch_A_2	A	6	6	6	6	Controlador_A_2 porta 0b
FC_switch_A_2	A	6	8	8	8	bridge_A_1a FC2
FC_switch_B_2	B	8	2	2	2	Controlador_B_1 porta 0b
FC_switch_B_2	B	8	6	6	6	Controlador_B_2 porta 0b

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2:

Switch FC	Local	Mudar de domínio	6505 / 6510 / G610	6520	G620	Liga a…
FC_switch_A_2	A	6	3	3	3	Controlador_A_1 porta 0d
FC_switch_A_2	A	6	7	7	7	Controlador_A_2 porta 0d
FC_switch_A_2	A	6	9	9	9	bridge_A_1b FC2
FC_switch_B_2	B	8	3	3	3	Controlador_B_1 porta 0d
FC_switch_B_2	B	8	7	7	7	Controlador_B_2 porta 0d

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9

Grupo DR 1 - pilha 2 no local_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…

FC_switch_A_1	A	5	2	2	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	6	6	6	Controlador_A_2 porta 0a
FC_switch_A_1	A	5	10	10	10	bridge_A_2a FC1
FC_switch_B_1	B	7	2	2	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	6	6	6	Controlador_B_2 porta 0a

Zona em tecido_1 hh	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	3	3	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	7	7	7	Controlador_A_2 porta 0C
FC_switch_A_1	A	5	11	11	11	bridge_A_2b FC1
FC_switch_B_1	B	7	3	3	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	7	7	7	Controlador_B_2 porta 0C

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…

FC_switch_A_2	A	6	2	0	0	Controlador_A_1 porta 0b
FC_switch_A_2	A	6	6	4	4	Controlador_A_2 porta 0b
FC_switch_A_2	A	6	10	10	10	bridge_A_2a FC2
FC_switch_B_2	B	8	2	2	2	Controlador_B_1 porta 0b
FC_switch_B_2	B	8	6	6	6	Controlador_B_2 porta 0b

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	3	3	3	Controlador_A_1 porta 0d
FC_switch_A_2	A	6	7	7	7	Controlador_A_2 porta 0d
FC_switch_A_2	A	6	11	11	11	bridge_A_2b FC2
FC_switch_B_2	B	8	3	3	3	Controlador_B_1 porta 0d
FC_switch_B_2	B	8	7	7	7	Controlador_B_2 porta 0d

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11

Grupo DR 1 - pilha 1 no local_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	2	2	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	6	6	6	Controlador_A_2 porta 0a
FC_switch_B_1	B	7	2	2	8	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	6	6	2	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	8	8	6	bridge_B_1a FC1

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	3	3	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	7	7	7	Controlador_A_2 porta 0C
FC_switch_B_1	B	7	3	3	9	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	7	7	3	Controlador_B_2 porta 0C
FC_switch_B_1	B	7	9	9	7	bridge_B_1b FC1

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	2	2	2	Controlador_A_1 porta 0b
FC_switch_A_2	A	6	6	6	6	Controlador_A_2 porta 0b
FC_switch_B_2	B	8	2	2	2	Controlador_B_1 porta 0b
FC_switch_B_2	B	8	6	6	6	Controlador_B_2 porta 0b
FC_switch_B_2	B	8	8	8	8	bridge_B_1a FC2

Zona em tecido_1	**Portos membros**
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	3	3	3	Controlador_A_1 porta 0d
FC_switch_A_2	A	6	7	7	7	Controlador_A_2 porta 0d
FC_switch_B_2	B	8	3	3	3	Controlador_B_1 porta 0d
FC_switch_B_2	B	8	7	7	7	Controlador_B_2 porta 0d
FC_switch_B_2	B	8	9	9	9	bridge_A_1b FC2

Zona em tecido_2	Portos membros
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

Grupo DR 1 - pilha 2 no local_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	2	2	2	Controlador_A_1 porta 0a
FC_switch_A_1	A	5	6	6	6	Controlador_A_2 porta 0a
FC_switch_B_1	B	7	2	2	2	Controlador_B_1 porta 0a
FC_switch_B_1	B	7	6	6	6	Controlador_B_2 porta 0a
FC_switch_B_1	B	7	10	10	10	bridge_B_2a FC1

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_1	A	5	3	3	3	Controlador_A_1 porta 0C
FC_switch_A_1	A	5	7	7	7	Controlador_A_2 porta 0C
FC_switch_B_1	B	7	3	3	3	Controlador_B_1 porta 0C
FC_switch_B_1	B	7	7	7	7	Controlador_B_2 porta 0C
FC_switch_B_1	B	7	11	11	11	bridge_B_2b FC1

Zona em tecido_2 hh	Portos membros

MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	2	2	2	Controlador_A_1 porta 0b
FC_switch_A_2	A	6	6	6	6	Controlador_A_2 porta 0b
FC_switch_B_2	B	8	2	2	2	Controlador_B_1 porta 0b
FC_switch_B_2	B	8	6	6	6	Controlador_B_2 porta 0b
FC_switch_B_2	B	8	10	10	10	bridge_B_2a FC2

Zona em tecido_1	Portos membros
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2:

Switch FC	Local	Mudar de domínio	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Liga a…
FC_switch_A_2	A	6	3	3	3	Controlador_A_1 porta 0d
FC_switch_A_2	A	6	7	7	7	Controlador_A_2 porta 0d
FC_switch_B_2	B	8	3	3	3	Controlador_B_1 porta 0d
FC_switch_B_2	B	8	7	7	7	Controlador_B_2 porta 0d
FC_switch_B_2	B	8	11	11	11	bridge_B_2b FC2

Zona em tecido_2	Portos membros

MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Resumo das zonas de armazenamento

Malha	Nome da zona	Portos membros
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Configuração de zoneamento em switches Brocade FC

É necessário atribuir as portas do switch a zonas separadas para separar o tráfego de storage e controlador, com zonas para as portas FC-VI e zonas para as portas de storage.

Sobre esta tarefa

As etapas a seguir usam o zoneamento padrão para a configuração do MetroCluster.

"Zoneamento para portas FC-VI"

"Zoneamento para pontes FibreBridge 7500N ou 7600N usando uma porta FC"

"Zoneamento para pontes FibreBridge 7500N usando ambas as portas FC"

Passos

1. Crie as zonas FC-VI em cada switch:

   ```
   zonecreate "QOSH1_FCVI_1", member;member …
   ```

   Neste exemplo, é criada uma zona FCVI DE QOS contendo as portas 5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5:

   ```
   Switch_A_1:admin> zonecreate "QOSH1_FCVI_1",
   "5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
   ```

2. Configure as zonas de armazenamento em cada switch.

   Você pode configurar o zoneamento para a malha a partir de um switch na malha. No exemplo a seguir, o zoneamento é configurado no Switch_A_1.

   a. Crie a zona de armazenamento para cada domínio do switch na malha do switch:

      ```
      zonecreate name, member;member …
      ```

      Neste exemplo, uma zona de armazenamento para um FibreBridge 7500N usando ambas as portas FC está sendo criada. As zonas contêm as portas 5,2;5,6;7,2;7,6;5,16:

      ```
      Switch_A_1:admin> zonecreate
      "MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
      ```

   b. Crie a configuração na primeira malha de switch:

      ```
      cfgcreate config_name, zone;zone…
      ```

Neste exemplo, é criada uma configuração com o nome CFG_1 e as duas zonas QOSH1_MC1_FAB_1_FCVI e MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1

```
Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
```

c. Adicione zonas à configuração, se desejar:

`cfgadd config_namezone;zone…`

d. Ativar a configuração:

`cfgenable config_name`

```
Switch_A_1:admin> cfgenable "CFG_1"
```

e. Guardar a configuração:

`cfgsave`

```
Switch_A_1:admin> cfgsave
```

f. Valide a configuração de zoneamento:

`zone --validate`

```
Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
-----------------------------------
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone
```

Definição da encriptação ISL em comutadores Brocade 6510 ou G620

Nos switches Brocade 6510 ou G620, você pode usar opcionalmente o recurso de criptografia Brocade nas conexões ISL. Se você quiser usar o recurso de criptografia, execute etapas de configuração adicionais em cada switch na configuração do MetroCluster.

Antes de começar

- Você deve ter switches Brocade 6510 ou G620.

> O suporte para criptografia ISL em switches Brocade G620 só é suportado no ONTAP 9.4 e posterior.

- Você deve ter selecionado dois switches da mesma malha.
- Você deve ter revisado a documentação do Brocade para a versão do sistema operacional de malha e switch para confirmar os limites de largura de banda e porta.

Sobre esta tarefa

As etapas devem ser executadas em ambos os switches na mesma malha.

Desativação da malha virtual

Para definir a criptografia ISL, você deve desativar a malha virtual em todos os quatro switches que estão sendo usados em uma configuração do MetroCluster.

Passos

1. Desative a malha virtual digitando o seguinte comando no console do switch:

   ```
   fosconfig --disable vf
   ```

2. Reinicie o switch.

Definir a carga útil

Após desativar a malha virtual, você deve definir a carga útil ou o tamanho do campo de dados em ambos os switches da malha.

Sobre esta tarefa

O tamanho do campo de dados não deve exceder 2048.

Passos

1. Desativar o interrutor:

   ```
   switchdisable
   ```

2. Configure e defina a carga útil:

   ```
   configure
   ```

3. Defina os seguintes parâmetros do interrutor:
   a. Defina o parâmetro Fabric da seguinte forma: `y`
   b. Defina os outros parâmetros, como domínio, PID persistente baseado em WWN, e assim por diante.
   c. Defina o tamanho do campo de dados: `2048`

Definir a política de autenticação

Você deve definir a política de autenticação e os parâmetros associados.

Sobre esta tarefa

Os comandos devem ser executados no console do switch.

Passos

1. Defina o segredo de autenticação:
   a. Inicie o processo de configuração:

      ```
      secAuthSecret --set
      ```

   Este comando inicia uma série de prompts que você responde nas seguintes etapas:

a. Forneça o nome mundial (WWN) do outro switch na malha para o parâmetro "Enter peer WWN, Domain ou switch name".
b. Forneça o segredo do par para o parâmetro "Enter peer secret".
c. Forneça o segredo local para o parâmetro "Enter local secret".
d. Introduza `Y` para o parâmetro "are you done".

   O seguinte é um exemplo de configuração do segredo de autenticação:

```
brcd> secAuthSecret --set

This command is used to set up secret keys for the DH-CHAP
authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is
performed
whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using
an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):
10:00:00:05:33:76:2e:99
Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] yes
Saving data to key store... Done.
```

2. Defina o grupo de autenticação como 4:

```
authUtil --set -g 4
```

3. Defina o tipo de autenticação como "dhchap":

```
authUtil --set -a dhchap
```

O sistema exibe a seguinte saída:

```
Authentication is set to dhchap.
```

4. Defina a política de autenticação no switch como On (ligado):

```
authUtil --policy -sw on
```

O sistema exibe a seguinte saída:

```
Warning: Activating the authentication policy requires either DH-CHAP
secrets or PKI certificates depending on the protocol selected.
Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE  (yes, y, no, n): [no] yes
Auth Policy is set to ON
```

Ativar a encriptação ISL em comutadores Brocade

Depois de definir a política de autenticação e o segredo de autenticação, você deve ativar a criptografia ISL nas portas para que ela entre em vigor.

Sobre esta tarefa

- Essas etapas devem ser executadas em uma malha de switch de cada vez.
- Os comandos devem ser executados no console do switch.

Passos

1. Ativar encriptação em todas as portas ISL:

```
portCfgEncrypt --enable port_number
```

No exemplo a seguir, a criptografia é ativada nas portas 8 e 12:

```
portCfgEncrypt --enable 8

portCfgEncrypt --enable 12
```

2. Ativar o interrutor:

```
switchenable
```

3. Verifique se o ISL está funcionando e funcionando:

```
islshow
```

4. Verifique se a criptografia está ativada:

```
portenccompshow
```

O exemplo a seguir mostra que a criptografia está habilitada nas portas 8 e 12:

```
User Encryption
Port  configured     Active
----   ----------    ------
 8      yes          yes
 9      No           No
 10     No           No
 11     No           No
 12     yes          yes
```

O que fazer a seguir

Execute todas as etapas nos switches na outra malha em uma configuração do MetroCluster.

Configuração manual dos switches Cisco FC

Cada switch Cisco na configuração do MetroCluster deve ser configurado adequadamente para as conexões ISL e de armazenamento.

Antes de começar

Os requisitos a seguir se aplicam aos switches Cisco FC:

- Você deve usar quatro switches Cisco compatíveis do mesmo modelo com a mesma versão e licenciamento do NX-os.
- A configuração do MetroCluster requer quatro switches.

  Os quatro switches devem ser conectados em duas malhas de dois switches cada, com cada malha abrangendo ambos os locais.

- O switch deve suportar conetividade com o modelo ATTO FibreBridge.
- Não é possível usar a criptografia ou a compactação na malha de storage Cisco FC. Não é suportado na configuração MetroCluster.

No "Ferramenta de Matriz de interoperabilidade NetApp (IMT)", você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

Sobre esta tarefa

O seguinte requisito aplica-se às ligações ISL (Inter-Switch Link):

- Todos os ISLs devem ter o mesmo comprimento e a mesma velocidade em um tecido.

  Diferentes comprimentos de ISLs podem ser usados nos diferentes tecidos. A mesma velocidade deve ser usada em todos os tecidos.

O seguinte requisito aplica-se às ligações de armazenamento:

- Cada controlador de storage deve ter quatro portas do iniciador disponíveis para conexão às malhas do

switch.

Duas portas de iniciador devem ser conectadas de cada controlador de storage a cada malha.

Você pode configurar sistemas FAS8020, AFF8020, FAS8200 e AFF A300 com duas portas de iniciadores por controladora (uma única porta de iniciador para cada malha) se todos os critérios a seguir forem atendidos:

- Há menos de quatro portas do iniciador FC disponíveis para conetar o armazenamento de disco e nenhuma porta adicional pode ser configurada como iniciadores FC.
- Todos os slots estão em uso e nenhuma placa de iniciador FC pode ser adicionada.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de licença de switch Cisco

Certas licenças baseadas em recursos podem ser necessárias para os switches Cisco em uma configuração MetroCluster conetada à malha. Essas licenças permitem que você use recursos como QoS ou créditos de modo de longa distância nos switches. Você deve instalar as licenças baseadas em recursos necessárias em todos os quatro switches em uma configuração do MetroCluster.

As seguintes licenças baseadas em recursos podem ser necessárias em uma configuração do MetroCluster:

- ENTERPRISE_PKG

  Essa licença permite que você use o recurso QoS em switches Cisco.

- PORT_ACTIVATION_PKG

  Você pode usar esta licença para switches Cisco 9148. Esta licença permite-lhe ativar ou desativar portas nos switches, desde que apenas 16 portas estejam ativas a qualquer momento. Por padrão, as portas 16 são habilitadas nos switches Cisco MDS 9148.

- FM_SERVER_PKG

  Essa licença permite que você gerencie malhas simultaneamente e gerencie switches por meio de um navegador da Web.

  A licença FM_Server_PKG também permite recursos de gerenciamento de desempenho, como limites de desempenho e monitoramento de limites. Para obter mais informações sobre essa licença, consulte o Pacote de servidor do Gerenciador de malha do Cisco.

Você pode verificar se as licenças estão instaladas usando o comando show license use. Se não tiver estas licenças, contacte o seu representante de vendas antes de prosseguir com a instalação.

Os switches Cisco MDS 9250i têm duas portas fixas de serviços de storage IP de 1/10 GbE. Não são necessárias licenças adicionais para estas portas. O pacote de aplicativos Cisco SAN Extension over IP é uma licença padrão nesses switches que permite recursos como FCIP e compactação.

Definir o switch Cisco FC para os padrões de fábrica

Para garantir uma configuração bem-sucedida, você deve definir o switch para seus padrões de fábrica. Isso garante que o switch esteja começando a partir de uma configuração limpa.

Sobre esta tarefa

Esta tarefa deve ser executada em todos os switches na configuração do MetroCluster.

Passos

1. Faça uma conexão de console e faça login em ambos os switches na mesma malha.
2. Volte a colocar o interrutor nas predefinições:

   `write erase`

   Você pode responder "y" quando solicitado a confirmar o comando. Isso apaga todas as licenças e informações de configuração no switch.

3. Reinicie o switch:

   `reload`

   Você pode responder "y" quando solicitado a confirmar o comando.

4. Repita os `write erase` comandos e `reload` no outro interrutor.

   Depois de emitir o `reload` comando, o switch reinicializa e, em seguida, solicita as perguntas de configuração. Nesse ponto, prossiga para a próxima seção.

Exemplo

O exemplo a seguir mostra o processo em uma malha que consiste em FC_switch_A_1 e FC_switch_B_1.

```
FC_Switch_A_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_A_1# reload
    This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_B_1# reload
    This command will reboot the system. (y/n)?  [n] y
```

Configure as configurações básicas do switch Cisco FC e a cadeia de carateres da comunidade

Você deve especificar as configurações básicas com o `setup` comando ou depois de emitir o `reload` comando.

Passos

1. Se o switch não exibir as perguntas de configuração, configure as configurações básicas do switch:

   ```
   setup
   ```

2. Aceite as respostas padrão às perguntas de configuração até que você seja solicitado a fornecer a string da comunidade SNMP.
3. Defina a cadeia de carateres da comunidade como "'public'" (todas minúsculas) para permitir o acesso a partir dos monitores de saúde do ONTAP.

   Você pode definir a cadeia de carateres da comunidade para um valor diferente de "público", mas você deve configurar os monitores de integridade do ONTAP usando a cadeia de carateres da comunidade especificada.

   O exemplo a seguir mostra os comandos em FC_switch_A_1:

   ```
   FC_switch_A_1# setup
       Configure read-only SNMP community string (yes/no) [n]: y
       SNMP community string : public
       Note:  Please set the SNMP community string to "Public" or another
   value of your choosing.
       Configure default switchport interface state (shut/noshut) [shut]:
   noshut
       Configure default switchport port mode F (yes/no) [n]: n
       Configure default zone policy (permit/deny) [deny]: deny
       Enable full zoneset distribution? (yes/no) [n]: yes
   ```

   O exemplo a seguir mostra os comandos em FC_switch_B_1:

   ```
   FC_switch_B_1# setup
       Configure read-only SNMP community string (yes/no) [n]: y
       SNMP community string : public
       Note:  Please set the SNMP community string to "Public" or another
   value of your choosing.
       Configure default switchport interface state (shut/noshut) [shut]:
   noshut
       Configure default switchport port mode F (yes/no) [n]: n
       Configure default zone policy (permit/deny) [deny]: deny
       Enable full zoneset distribution? (yes/no) [n]: yes
   ```

Adquirir licenças para portas

Você não precisa usar licenças de switch Cisco em um intervalo contínuo de portas; em vez disso, você pode adquirir licenças para portas específicas que são usadas e remover licenças de portas não utilizadas.

Antes de começar

Você deve verificar o número de portas licenciadas na configuração do switch e, se necessário, mover licenças de uma porta para outra, conforme necessário.

Passos

1. Exibir o uso da licença para uma estrutura de switch:

   ```
   show port-resources module 1
   ```

   Determine quais portas exigem licenças. Se algumas dessas portas não forem licenciadas, determine se você tem portas licenciadas extras e considere remover as licenças delas.

2. Entre no modo de configuração:

   ```
   config t
   ```

3. Remova a licença da porta selecionada:
   a. Selecione a porta a ser não licenciada:

      ```
      interface interface-name
      ```

   b. Remova a licença da porta:

      ```
      no port-license acquire
      ```

   c. Saia da interface de configuração da porta:

      ```
      exit
      ```

4. Adquira a licença para a porta selecionada:
   a. Selecione a porta a ser não licenciada:

      ```
      interface interface-name
      ```

   b. Torne a porta elegível para adquirir uma licença:

      ```
      port-license
      ```

   c. Adquira a licença na porta:

      ```
      port-license acquire
      ```

   d. Saia da interface de configuração da porta:

      ```
      exit
      ```

5. Repita para quaisquer portas adicionais.
6. Sair do modo de configuração:

   ```
   exit
   ```

Removendo e adquirindo uma licença em uma porta

Este exemplo mostra uma licença que está sendo removida da porta FC1/2, a porta FC1/1 que está sendo elegível para adquirir uma licença e a licença que está sendo adquirida na porta FC1/1:

```
Switch_A_1# conf t
    Switch_A_1(config)# interface fc1/2
    Switch_A_1(config)# shut
    Switch_A_1(config-if)# no port-license acquire
    Switch_A_1(config-if)# exit
    Switch_A_1(config)# interface fc1/1
    Switch_A_1(config-if)# port-license
    Switch_A_1(config-if)# port-license acquire
    Switch_A_1(config-if)# no shut
    Switch_A_1(config-if)# end
    Switch_A_1# copy running-config startup-config

    Switch_B_1# conf t
    Switch_B_1(config)# interface fc1/2
    Switch_B_1(config)# shut
    Switch_B_1(config-if)# no port-license acquire
    Switch_B_1(config-if)# exit
    Switch_B_1(config)# interface fc1/1
    Switch_B_1(config-if)# port-license
    Switch_B_1(config-if)# port-license acquire
    Switch_B_1(config-if)# no shut
    Switch_B_1(config-if)# end
    Switch_B_1# copy running-config startup-config
```

O exemplo a seguir mostra o uso da licença de porta sendo verificado:

```
Switch_A_1# show port-resources module 1
    Switch_B_1# show port-resources module 1
```

Habilitando portas em um switch Cisco MDS 9148 ou 9148S

Nos switches Cisco MDS 9148 ou 9148S, é necessário habilitar manualmente as portas necessárias em uma configuração do MetroCluster.

Sobre esta tarefa

- Você pode ativar manualmente portas 16 em um switch Cisco MDS 9148 ou 9148S.
- Os switches Cisco permitem que você aplique a licença DO POD em portas aleatórias, em vez de aplicá-las em sequência.
- Os switches Cisco exigem que você use uma porta de cada grupo de portas, a menos que você precise de mais de 12 portas.

Passos

1. Veja os grupos de portas disponíveis em um switch Cisco:

   `show port-resources module` *`blade_number`*

2. Licencie e adquira a porta necessária em um grupo de portas:

   ```
   config t

   interface port_number

   shut

   port-license acquire

   no shut
   ```

   Por exemplo, a seguinte sequência de comandos licencia e adquire a porta fc 1/45:

   ```
   switch# config t
   switch(config)#
   switch(config)# interface fc 1/45
   switch(config-if)#
   switch(config-if)# shut
   switch(config-if)# port-license acquire
   switch(config-if)# no shut
   switch(config-if)# end
   ```

3. Guardar a configuração:

   ```
   copy running-config startup-config
   ```

Configurando as portas F em um switch Cisco FC

Você deve configurar as portas F no switch FC.

Sobre esta tarefa

Em uma configuração MetroCluster, as portas F são as portas que conetam o switch aos iniciadores HBA, interconexões FC-VI e pontes FC-para-SAS.

Cada porta deve ser configurada individualmente.

Consulte as seções a seguir para identificar as portas F (switch-to-node) para sua configuração:

- "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Esta tarefa deve ser executada em cada switch na configuração do MetroCluster.

Passos

1. Entre no modo de configuração:

   ```
   config t
   ```

2. Entre no modo de configuração da interface para a porta:

```
interface port-ID
```

3. Desligue a porta:

```
shutdown
```

4. Defina as portas para o modo F:

```
switchport mode F
```

5. Defina as portas para velocidade fixa:

```
switchport speed speed-value
```

speed-value é `8000` ou `16000`

6. Defina o modo de taxa da porta do switch para dedicado:

```
switchport rate-mode dedicated
```

7. Reinicie a porta:

```
no shutdown
```

8. Sair do modo de configuração:

```
end
```

Exemplo

O exemplo a seguir mostra os comandos nos dois switches:

```
Switch_A_1# config  t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config  t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

Atribuição de créditos de buffer a buffer a portas F no mesmo grupo de portas que o ISL

Você deve atribuir os créditos buffer a buffer às portas F se estiverem no mesmo grupo de portas que o ISL. Se as portas não tiverem os créditos buffer-to-buffer necessários, o ISL pode estar inoperacional.

Sobre esta tarefa

Esta tarefa não é necessária se as portas F não estiverem no mesmo grupo de portas que a porta ISL.

Se as portas F estiverem em um grupo de portas que contenha o ISL, essa tarefa deve ser executada em cada switch FC na configuração do MetroCluster.

Passos

1. Entre no modo de configuração:

   ```
   config t
   ```

2. Defina o modo de configuração da interface para a porta:

   ```
   interface port-ID
   ```

3. Desative a porta:

   ```
   shut
   ```

4. Se a porta ainda não estiver no modo F, defina a porta para o modo F:

   ```
   switchport mode F
   ```

5. Defina o crédito buffer-to-buffer das portas não e como 1:

   ```
   switchport fcrxbbcredit 1
   ```

6. Reative a porta:

   ```
   no shut
   ```

7. Sair do modo de configuração:

   ```
   exit
   ```

8. Copie a configuração atualizada para a configuração de inicialização:

   ```
   copy running-config startup-config
   ```

9. Verifique o crédito buffer-to-buffer atribuído a uma porta:

   ```
   show port-resources module 1
   ```

10. Sair do modo de configuração:

    ```
    exit
    ```

11. Repita estes passos no outro interrutor do tecido.
12. Verifique as configurações:

```
show port-resource module 1
```

Exemplo

Neste exemplo, a porta FC1/40 é o ISL. As portas FC1/37, FC1/38 e FC1/39 estão no mesmo grupo de portas e devem ser configuradas.

Os comandos a seguir mostram o intervalo de portas que está sendo configurado para FC1/37 até FC1/39:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

Os comandos a seguir e a saída do sistema mostram que as configurações são aplicadas corretamente:

```
FC_switch_A_1# show port-resource module 1
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                      Buffers     (Gbps)

--------------------------------------------------------------------------
fc1/37                                    32        8.0  dedicated
fc1/38                                     1        8.0  dedicated
fc1/39                                     1        8.0  dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                    Buffers     (Gbps)

--------------------------------------------------------------------------
fc1/37                                    32        8.0  dedicated
fc1/38                                     1        8.0  dedicated
fc1/39                                     1        8.0 dedicated
...
```

Criando e configurando VSANs em switches Cisco FC

É necessário criar um VSAN para as portas FC-VI e um VSAN para as portas de storage em cada switch FC na configuração MetroCluster.

Sobre esta tarefa

Os VSANs devem ter um número e um nome exclusivos. Você deve fazer uma configuração adicional se estiver usando dois ISLs com entrega em ordem de quadros.

Os exemplos desta tarefa usam as seguintes convenções de nomenclatura:

Malha de switch	Nome VSAN	Número de ID
1	FCVI_1_10	10
STOR_1_20	20	2

FCVI_2_30	30	STOR_2_20

Essa tarefa deve ser executada em cada malha de switch FC.

Passos

1. Configure o FC-VI VSAN:
   a. Entre no modo de configuração se ainda não o tiver feito:

      ```
      config t
      ```

   b. Edite o banco de dados VSAN:

      ```
      vsan database
      ```

   c. Defina a ID VSAN:

      ```
      vsan vsan-ID
      ```

   d. Defina o nome VSAN:

      ```
      vsan vsan-ID name vsan_name
      ```

2. Adicionar portas ao VSAN FC-VI:
   a. Adicione as interfaces para cada porta no VSAN:

      ```
      vsan vsan-ID interface interface_name
      ```

      Para o VSAN FC-VI, as portas que conetam as portas FC-VI locais serão adicionadas.

   b. Sair do modo de configuração:

      ```
      end
      ```

   c. Copie o running-config para o startup-config:

      ```
      copy running-config startup-config
      ```

      No exemplo a seguir, as portas são FC1/1 e FC1/13:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

3. Verifique a associação da porta do VSAN:

   `show vsan member`

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

4. Configure o VSAN para garantir a entrega em ordem de quadros ou entrega fora de ordem de quadros:

   As configurações padrão de IOD são recomendadas. Você deve configurar ODE somente se necessário.

   "Considerações sobre o uso de equipamentos TDM/WDM com configurações MetroCluster conetadas à malha"

   - As etapas a seguir devem ser executadas para configurar a entrega em ordem de quadros:

     i. Entre no modo de configuração:

        `conf t`

     ii. Ativar a garantia em ordem das trocas para o VSAN:

        `in-order-guarantee vsan` *`vsan-ID`*

        Para VSANs FC-VI (FCVI_1_10 e FCVI_2_30), você deve habilitar a garantia em ordem de quadros e trocas somente no VSAN 10.

     iii. Ative o balanceamento de carga para o VSAN:

        `vsan` *`vsan-ID`* `loadbalancing src-dst-id`

     iv. Sair do modo de configuração:

        `end`

v. Copie o running-config para o startup-config:

```
copy running-config startup-config
```

Os comandos para configurar a entrega em ordem de quadros em FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Os comandos para configurar a entrega em ordem de quadros em FC_switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

◦ As etapas a seguir devem ser executadas para configurar a entrega fora do pedido de quadros:

i. Entre no modo de configuração:

```
conf t
```

ii. Desative a garantia de troca por encomenda para o VSAN:

```
no in-order-guarantee vsan vsan-ID
```

iii. Ative o balanceamento de carga para o VSAN:

```
vsan vsan-ID loadbalancing src-dst-id
```

iv. Sair do modo de configuração:

```
end
```

v. Copie o running-config para o startup-config:

```
copy running-config startup-config
```

Os comandos para configurar a entrega fora de ordem de quadros em FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Os comandos para configurar a entrega fora de ordem de quadros em FC_switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

+

Ao configurar o ONTAP nos módulos do controlador, O AID deve ser explicitamente configurado em cada módulo do controlador na configuração do MetroCluster.

"Configuração da entrega em ordem ou entrega fora de ordem de quadros no software ONTAP"

5. Defina políticas de QoS para o VSAN FC-VI:
   a. Entre no modo de configuração:

      `conf t`

   b. Ative a QoS e crie um mapa de classes inserindo os seguintes comandos em sequência:

      `qos enable`

      `qos class-map` *`class_name`* `match-any`

   c. Adicione o mapa de classe criado em uma etapa anterior ao mapa de políticas:

      `class` *`class_name`*

   d. Defina a prioridade:

      `priority high`

   e. Adicione o VSAN ao mapa de políticas criado anteriormente neste procedimento:

      `qos service policy` *`policy_name`* `vsan` *`vsan-id`*

   f. Copie a configuração atualizada para a configuração de inicialização:

```
copy running-config startup-config
```

Os comandos para definir as políticas de QoS em FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

Os comandos para definir as políticas de QoS em FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. Configurar o armazenamento VSAN:

   a. Defina a ID VSAN:

      `vsan *vsan-ID*`

   b. Defina o nome VSAN:

      `vsan *vsan-ID* name *vsan_name*`

Os comandos para configurar o VSAN de armazenamento em FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Os comandos para configurar o VSAN de armazenamento em FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

7. Adicione portas ao VSAN de armazenamento.

   Para o VSAN de storage, todas as portas que conectam pontes HBA ou FC a SAS devem ser adicionadas. Neste exemplo FC1/5, FC1/FC1, FC1/17, FC1/21. FC1/25, FC1/29, 9/33 e FC1/37 estão sendo adicionados.

   Os comandos para adicionar portas ao VSAN de armazenamento em FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

   Os comandos para adicionar portas ao VSAN de armazenamento em FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

Configurando portas e

Você deve configurar as portas do switch que conetam o ISL (estas são as portas e).

Sobre esta tarefa

O procedimento utilizado depende do interrutor que está a utilizar:

- Configuração das portas e no switch Cisco FC
- Configuração de portas FCIP para um único ISL em switches FC Cisco 9250i
- Configuração de portas FCIP para um ISL duplo em switches FC Cisco 9250i

Configuração das portas e no switch Cisco FC

Você deve configurar as portas do switch FC que conetam o link inter-switch (ISL).

Sobre esta tarefa

Estas são as portas e, e a configuração deve ser feita para cada porta. Para fazer isso, você deve calcular o número correto de créditos de buffer a buffer (BBCs).

Todos os ISLs na malha devem ser configurados com as mesmas configurações de velocidade e distância.

Esta tarefa deve ser executada em cada porta ISL.

Passos

1. Use a tabela a seguir para determinar as BBCs necessárias ajustadas por quilômetro para possíveis velocidades da porta.

   Para determinar o número correto de BBCs, multiplique as BBCs ajustadas necessárias (determinadas a partir da tabela a seguir) pela distância em quilômetros entre os switches. Um fator de ajuste de 1,5 é necessário para considerar o comportamento de enquadramento FC-VI.

Velocidade em Gbps	BBCs necessários por quilômetro	BBCs ajustados necessários (BBCs por km x 1,5)
1	0,5	0,75

2	1	1,5
4	2	3
8	4	6
16	8	12

Por exemplo, para calcular o número necessário de créditos para uma distância de 30 km em um link de 4 Gbps, faça o seguinte cálculo:

- `Speed in Gbps` é 4
- `Adjusted BBCs required` é 3
- `Distance in kilometers between switches` é de 30 km
- 3 x 30: 90

a. Entre no modo de configuração:

```
config t
```

b. Especifique a porta que você está configurando:

```
interface port-name
```

c. Desligue a porta:

```
shutdown
```

d. Defina o modo de taxa da porta para "dedicado":

```
switchport rate-mode dedicated
```

e. Defina a velocidade para a porta:

```
switchport speed speed-value
```

f. Defina os créditos buffer-to-buffer para a porta:

```
switchport fcrxbbcredit number_of_buffers
```

g. Defina a porta para o modo e:

```
switchport mode E
```

h. Ative o modo de tronco para a porta:

```
switchport trunk mode on
```

i. Adicione as redes de área de armazenamento virtual ISL (VSANs) ao tronco:

```
switchport trunk allowed vsan 10

switchport trunk allowed vsan add 20
```

j. Adicione a porta ao canal de porta 1:

```
channel-group 1
```

k. Repita as etapas anteriores para a porta ISL correspondente no switch parceiro na malha.

O exemplo a seguir mostra a porta FC1/41 configurada para uma distância de 30 km e 8 Gbps:

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

l. Execute o seguinte comando em ambos os switches para reiniciar as portas:

```
no shutdown
```

m. Repita os passos anteriores para as outras portas ISL na estrutura.

n. Adicione o VSAN nativo à interface de canal de porta em ambos os switches na mesma estrutura:

```
interface port-channel number

switchport trunk allowed vsan add native_san_id
```

o. Verifique a configuração do canal de porta:

```
show interface port-channel number
```

O canal da porta deve ter os seguintes atributos:

- O canal de porta é "entroncamento".
- O modo de porta de administrador é e, o modo de tronco está ativado.
- Speed (velocidade) mostra o valor cumulativo de todas as velocidades de ligação ISL.

  Por exemplo, duas portas ISL operando a 4 Gbps devem mostrar uma velocidade de 8 Gbps.

- `Trunk vsans (admin allowed and active)` Mostra todos os VSANs permitidos.
- `Trunk vsans (up)` Mostra todos os VSANs permitidos.
- A lista de membros mostra todas as portas ISL que foram adicionadas ao canal de porta.
- O número VSAN da porta deve ser o mesmo que o VSAN que contém os ISLs (normalmente vsan 1 nativo).

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
    Hardware is Fibre Channel
    Port WWN is 24:01:54:7f:ee:e2:8d:a0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,10,20)
    Trunk vsans (up)                       (1,10,20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
    5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
      535724861 frames input,1069616011292 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      572290295 frames output,1144869385204 bytes
        0 discards,0 errors
      5 input OLS,11  LRR,2 NOS,0 loop inits
      14 output OLS,5 LRR, 0 NOS, 0 loop inits
    Member[1] : fc1/36
    Member[2] : fc1/40
    Interface last changed at Thu Oct 16 11:48:00 2014
```

a. Sair da configuração da interface em ambos os switches:

```
end
```

b. Copie a configuração atualizada para a configuração de inicialização em ambas as malhas:

```
copy running-config startup-config
```

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

a. Repita os passos anteriores no segundo tecido do interrutor.

Informações relacionadas

Você precisa verificar se está usando as atribuições de portas especificadas quando você faz o cabeamento dos switches FC ao usar o ONTAP 9.1 e posterior. Consulte "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Configuração de portas FCIP para um único ISL em switches FC Cisco 9250i

Você deve configurar as portas do switch FCIP que conetam o ISL (e-ports) criando perfis e interfaces FCIP e atribuindo-os à interface IPStorage1/1 GbE.

Sobre esta tarefa

Esta tarefa é apenas para configurações que usam um único ISL por malha de switch, usando a interface IPStorage1/1 em cada switch.

Essa tarefa deve ser executada em cada switch FC.

Dois perfis FCIP são criados em cada switch:

- Tecido 1
  - FC_switch_A_1 é configurado com os perfis FCIP 11 e 111.
  - FC_switch_B_1 é configurado com os perfis FCIP 12 e 121.
- Tecido 2
  - FC_switch_A_2 é configurado com os perfis FCIP 13 e 131.
  - FC_switch_B_2 é configurado com os perfis FCIP 14 e 141.

Passos

1. Entre no modo de configuração:

```
config t
```

2. Ativar FCIP:

```
feature fcip
```

3. Configure a interface IPStorage1/1 GbE:

   a. Entre no modo de configuração:

      ```
      conf t
      ```

   b. Especifique a interface IPStorage1/1:

      ```
      interface IPStorage1/1
      ```

   c. Especifique o endereço IP e a máscara de sub-rede:

      ```
      interface ip-address subnet-mask
      ```

   d. Especifique o tamanho da MTU de 2500:

      ```
      switchport mtu 2500
      ```

   e. Ativar a porta:

      ```
      no shutdown
      ```

   f. Sair do modo de configuração:

      ```
      exit
      ```

   O exemplo a seguir mostra a configuração de uma porta IPStorage1/1:

   ```
   conf t
   interface IPStorage1/1
     ip address 192.168.1.201 255.255.255.0
     switchport mtu 2500
     no shutdown
   exit
   ```

4. Configure o perfil FCIP para tráfego FC-VI:

   a. Configure um perfil FCIP e entre no modo de configuração do perfil FCIP:

      ```
      fcip profile FCIP-profile-name
      ```

      O nome do perfil depende de qual switch está sendo configurado.

   b. Atribua o endereço IP da interface IPStorage1/1 ao perfil FCIP:

      ```
      ip address ip-address
      ```

   c. Atribua o perfil FCIP à porta TCP 3227:

      ```
      port 3227
      ```

d. Defina as configurações TCP:

```
tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable``no tcp cwm
```

O exemplo a seguir mostra a configuração do perfil FCIP:

```
conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

5. Configure o perfil FCIP para o tráfego de armazenamento:

a. Configure um perfil FCIP com o nome 111 e entre no modo de configuração do perfil FCIP:

```
fcip profile 111
```

b. Atribua o endereço IP da interface IPStorage1/1 ao perfil FCIP:

```
ip address ip-address
```

c. Atribua o perfil FCIP à porta TCP 3229:

```
port 3229
```

d. Defina as configurações TCP:

```
tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable``no tcp cwm
```

O exemplo a seguir mostra a configuração do perfil FCIP:

```
conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

6. Crie a primeira de duas interfaces FCIP:

```
interface fcip 1
```

Esta interface é usada para tráfego FC-IV.

a. Selecione o perfil 11 criado anteriormente:

```
use-profile 11
```

b. Defina o endereço IP e a porta da porta IPStorage1/1 no switch parceiro:

```
peer-info ipaddr partner-switch-port-ip port 3227
```

c. Selecione a ligação TCP 2:

```
tcp-connection 2
```

d. Desativar compressão:

```
no ip-compression
```

e. Ativar a interface:

```
no shutdown
```

f. Configure a conexão TCP de controle para 48 e a conexão de dados para 26 para marcar todos os pacotes nesse valor DSCP (Differentiated Services Code Point):

```
qos control 48 data 26
```

g. Sair do modo de configuração da interface:

```
exit
```

O exemplo a seguir mostra a configuração da interface FCIP:

```
interface fcip  1
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.334   port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. Crie a segunda de duas interfaces FCIP:

```
interface fcip 2
```

Esta interface é usada para o tráfego de armazenamento.

a. Selecione o perfil 111 criado anteriormente:

```
use-profile 111
```

b. Defina o endereço IP e a porta da porta IPStorage1/1 no switch parceiro:

```
peer-info ipaddr partner-switch-port-ip port 3229
```

c. Selecione a ligação TCP 2:

```
tcp-connection 5
```

d. Desativar compressão:

```
no ip-compression
```

e. Ativar a interface:

```
no shutdown
```

f. Configure a conexão TCP de controle para 48 e conexão de dados para 26 para marcar todos os pacotes nesse valor de ponto de código de serviços diferenciados (DSCP):

```
qos control 48 data 26
```

g. Sair do modo de configuração da interface:

```
exit
```

O exemplo a seguir mostra a configuração da interface FCIP:

```
interface fcip  2
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.33e  port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. Configure as configurações de switchport na interface fcip 1:

a. Entre no modo de configuração:

```
config t
```

b. Especifique a porta que você está configurando:

```
interface fcip 1
```

c. Desligue a porta:

```
shutdown
```

d. Defina a porta para o modo e:

```
switchport mode E
```

e. Ative o modo de tronco para a porta:

```
switchport trunk mode on
```

f. Defina o tronco permitido vsan para 10:

```
switchport trunk allowed vsan 10
```

g. Defina a velocidade para a porta:

```
switchport speed speed-value
```

9. Configure as configurações de switchport na interface fcip 2:
   a. Entre no modo de configuração:

```
config t
```

   b. Especifique a porta que você está configurando:

```
interface fcip 2
```

   c. Desligue a porta:

```
shutdown
```

   d. Defina a porta para o modo e:

```
switchport mode E
```

   e. Ative o modo de tronco para a porta:

```
switchport trunk mode on
```

   f. Defina o tronco permitido vsan para 20:

```
switchport trunk allowed vsan 20
```

   g. Defina a velocidade para a porta:

```
switchport speed speed-value
```

10. Repita os passos anteriores no segundo interrutor.

    As únicas diferenças são os endereços IP apropriados e os nomes de perfil FCIP exclusivos.

    - Ao configurar a primeira malha de switch, FC_switch_B_1 é configurado com os perfis FCIP 12 e 121.
    - Ao configurar a primeira malha de switch, FC_switch_A_2 é configurado com os perfis FCIP 13 e 131 e FC_switch_B_2 é configurado com os perfis FCIP 14 e 141.

11. Reinicie as portas em ambos os switches:

```
no shutdown
```

12. Saia da configuração da interface em ambos os switches:

```
end
```

13. Copie a configuração atualizada para a configuração de inicialização em ambos os switches:

```
copy running-config startup-config
```

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

14. Repita os passos anteriores no segundo tecido do interrutor.

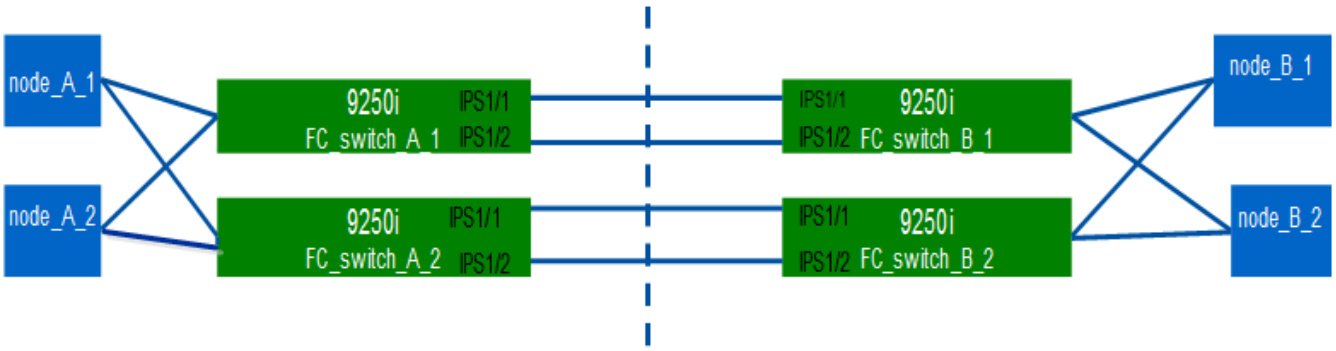
Configuração de portas FCIP para um ISL duplo em switches FC Cisco 9250i

Você deve configurar as portas do switch FCIP que conetam o ISL (e-ports) criando perfis e interfaces FCIP e atribuindo-os às interfaces IPStorage1/1 e IPStorage1/2 GbE.

Sobre esta tarefa

Essa tarefa é apenas para configurações que usam um ISL duplo por malha de switch, usando as interfaces IPStorage1/1 e IPStorage1/2 GbE em cada switch.

Essa tarefa deve ser executada em cada switch FC.



A tarefa e os exemplos usam as seguintes tabelas de configuração de perfil:

- [fabric1_table]
- [fabric2_table]
- Tabela de configuração de perfil de tecido 1 *

Malha de switch	Interface IPStorage	Endereço IP	Tipo de porta	Interface FCIP	Perfil FCIP	Porta	IP/porta peer	ID VSAN
FC_switch _A_1	IPStorage 1/1	a.a.a.a.	FC-VI	fcip 1	15	3220	c.c.c.c/323 0	10
Armazena mento	fcip 2	20	3221	c.c.c.c/323 1	20	IPStorage 1/2	b.b.b.b	FC-VI
fcip 3	25	3222	d.dd.d/323 2	10	Armazena mento	fcip 4	30	3223

d.dd.d/323 3	20	FC_switch _B_1	IPStorage 1/1	c.c.c.c	FC-VI	fcip 1	15	3230
a.a.a.a.a/3 220	10	Armazena mento	fcip 2	20	3231	a.a.a.a.a/3 221	20	IPStorage 1/2
d.d.d.d	FC-VI	fcip 3	25	3232	b.b.b.b/32 22	10	Armazena mento	fcip 4

- Tabela de configuração de perfil de tecido 2 *

Malha de switch	Interface IPStorage	Endereço IP	Tipo de porta	Interface FCIP	Perfil FCIP	Porta	IP/porta peer	ID VSAN
FC_switch _A_2	IPStorage 1/1	por exemplo	FC-VI	fcip 1	15	3220	1. g.g.g/3 230	10
Armazena mento	fcip 2	20	3221	1. g.g.g/3 231	20	IPStorage 1/2	f.f.f.f	FC-VI
fcip 3	25	3222	h.h.h.h. h/3232	10	Armazena mento	fcip 4	30	3223
h.h.h.h. h/3233	20	FC_switch _B_2	IPStorage 1/1	g.g.g.g	FC-VI	fcip 1	15	3230
e.e.e.e/32 20	10	Armazena mento	fcip 2	20	3231	e.e.e.e/32 21	20	IPStorage 1/2
h.h.h.h	FC-VI	fcip 3	25	3232	f.f. f/3222	10	Armazena mento	fcip 4

Passos

1. Entre no modo de configuração:

   ```
   config t
   ```

2. Ativar FCIP:

   ```
   feature fcip
   ```

3. Em cada switch, configure as duas interfaces IPStorage ("'IPStorage1/1" e "'IPStorage1/2"):

   a. entrar no modo de configuração:

      ```
      conf t
      ```

b. Especifique a interface IPStorage para criar:

```
interface ipstorage
```

O *ipstorage* valor do parâmetro é "'IPStorage1/1" ou "'IPStorage1/2".

c. Especifique o endereço IP e a máscara de sub-rede da interface IPStorage especificada anteriormente:

```
interface ip-address subnet-mask
```

> Em cada switch, as interfaces IPStorage "'IPStorage1/1" e "'IPStorage1/2" devem ter endereços IP diferentes.

a. Especifique o tamanho da MTU como 2500:

```
switchport mtu 2500
```

b. Ativar a porta:

```
no shutdown
```

c. Sair do modo de configuração:

```
exit
```

d. Repita substep "'a' até substep "'f' para configurar a interface IPStorage1/2 GbE com um endereço IP diferente.

4. Configure os perfis FCIP para FC-VI e tráfego de storage com os nomes de perfil fornecidos na tabela de configuração de perfil:

a. Entre no modo de configuração:

```
conf t
```

b. Configure os perfis FCIP com os seguintes nomes de perfil:

```
fcip profile FCIP-profile-name
```

A lista a seguir fornece os valores para o *FCIP-profile-name* parâmetro:

- 15 para FC-VI em IPStorage1/1
- 20 para armazenamento em IPStorage1/1
- 25 para FC-VI em IPStorage1/2
- 30 para armazenamento em IPStorage1/2

c. Atribua as portas do perfil FCIP de acordo com a tabela de configuração do perfil:

```
port port_number
```

d. Defina as configurações TCP:

```
tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable

no tcp cwm
```

5. Criar interfaces FCIP:

   `interface fcip FCIP_interface`

   O `FCIP_interface` valor do parâmetro é ""1"", ""2"", ""3"", ou ""4"", como mostrado na tabela de configuração do perfil.

   a. Mapeie interfaces para os perfis criados anteriormente:

      `use-profile profile`

   b. Defina o endereço IP de ponto e o número da porta do perfil de ponto:

      `peer-info peer IPstorage ipaddr port peer_profile_port_number`

   c. Selecione as conexões TCP:

      `tcp-connection connection-#`

   O `connection-#` valor do parâmetro é "'2'" para perfis FC-VI e "'5" para perfis de armazenamento.

   a. Desativar compressão:

      `no ip-compression`

   b. Ativar a interface:

      `no shutdown`

   c. Configure a conexão TCP de controle como "'48'" e a conexão de dados como "'26'" para marcar todos os pacotes que têm valor de ponto de código de serviços diferenciados (DSCP):

      `qos control 48 data 26`

   d. Sair do modo de configuração:

      `exit`

6. Configure as configurações de switchport em cada interface FCIP:

   a. Entre no modo de configuração:

      ```
      config t
      ```

   b. Especifique a porta que você está configurando:

      ```
      interface fcip 1
      ```

   c. Desligue a porta:

      ```
      shutdown
      ```

   d. Defina a porta para o modo e:

      ```
      switchport mode E
      ```

   e. Ative o modo de tronco para a porta:

      ```
      switchport trunk mode on
      ```

   f. Especifique o tronco permitido em um VSAN específico:

      ```
      switchport trunk allowed vsan vsan_id
      ```

   O valor do parâmetro *vsan_id* é "VSAN 10" para perfis FC-VI e "VSAN 20" para perfis de armazenamento.

   a. Defina a velocidade para a porta:

      ```
      switchport speed speed-value
      ```

   b. Sair do modo de configuração:

      ```
      exit
      ```

7. Copie a configuração atualizada para a configuração de inicialização em ambos os switches:

   ```
   copy running-config startup-config
   ```

Os exemplos a seguir mostram a configuração de portas FCIP para um ISL duplo em switches de malha 1 FC_switch_A_1 e FC_switch_B_1.

Para FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings
```

```
feature  fcip

conf t
interface IPStorage1/1
#  IP address:  a.a.a.a
#  Mask:  y.y.y.y
  ip address <a.a.a.a   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit
conf t
fcip profile 15
  ip address <a.a.a.a>
  port 3220
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <a.a.a.a>
  port 3221
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  b.b.b.b
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit
```

```
conf t
fcip profile 25
  ip address <b.b.b.b>
  port 3222
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <b.b.b.b>
  port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3230
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3231
  tcp-connection 5
  no ip-compression
```

```
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3232
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3233
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
```

```
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Para FC_switch_B_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  c.c.c.c
#  Mask:  y.y.y.y
  ip address <c.c.c.c   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 15
  ip address <c.c.c.c>
  port 3230
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
```

```
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  d.d.d.d
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233
```

```
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3220
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3221
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3222
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
```

```
listening on
 peer-info ipaddr < b.b.b.b >  port 3223
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Configurando o zoneamento em um switch Cisco FC

É necessário atribuir as portas do switch a zonas separadas para isolar o tráfego de storage (HBA) e controlador (FC-VI).

Sobre esta tarefa

Essas etapas devem ser executadas em ambas as malhas de switches FC.

As etapas a seguir usam o zoneamento descrito na seção Zoneamento para um FibreBridge 7500N em uma configuração de MetroCluster de quatro nós. "Zoneamento para portas FC-VI"Consulte a .

Passos

1. Limpe as zonas existentes e o conjunto de zonas, se existir.

   a. Determine quais zonas e conjuntos de zonas estão ativos:

      `show zoneset active`

      ```
      FC_switch_A_1# show zoneset active

      FC_switch_B_1# show zoneset active
      ```

   b. Desative os conjuntos de zonas ativas identificados na etapa anterior:

      `no zoneset activate name zoneset_name vsan vsan_id`

      O exemplo a seguir mostra dois conjuntos de zonas sendo desabilitados:

      - ZoneSet_A em FC_switch_A_1 no VSAN 10
      - ZoneSet_B no FC_switch_B_1 no VSAN 20

      ```
      FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10

      FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
      ```

   c. Depois de todos os conjuntos de zonas serem desativados, limpe a base de dados de zonas:

      `clear zone database zone-name`

   ```
   FC_switch_A_1# clear zone database 10
   FC_switch_A_1# copy running-config startup-config

   FC_switch_B_1# clear zone database 20
   FC_switch_B_1# copy running-config startup-config
   ```

2. Obtenha o nome mundial do switch (WWN):

```
show wwn switch
```

3. Configure as definições básicas de zona:

   a. Defina a política de zoneamento padrão como ""permissão"":

      ```
      no system default zone default-zone permit
      ```

   b. Ative a distribuição completa da zona:

      ```
      system default zone distribute full
      ```

   c. Defina a política de zoneamento padrão para cada VSAN:

      ```
      no zone default-zone permit vsanid
      ```

   d. Defina a distribuição de zona completa padrão para cada VSAN:

      ```
      zoneset distribute full vsanid
      ```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

4. Crie zonas de armazenamento e adicione as portas de armazenamento a elas.

   Execute estas etapas em apenas um switch em cada malha.

   O zoneamento depende do modelo de ponte FC-para-SAS que você está usando. Para obter detalhes, consulte a seção para sua ponte modelo. Os exemplos mostram portas de switch Brocade, então ajuste suas portas de acordo.

- "Zoneamento para pontes FibreBridge 7500N ou 7600N usando uma porta FC"
- "Zoneamento para pontes FibreBridge 7500N usando ambas as portas FC"

Cada zona de storage contém as portas do iniciador HBA de todos os controladores e uma única porta que conecta uma ponte FC a SAS.

a. Crie as zonas de armazenamento:

```
zone name STOR-zone-name vsan vsanid
```

b. Adicionar portas de armazenamento à zona:

```
member portswitch WWN
```

c. Ative o conjunto de zonas:

```
zoneset activate name STOR-zone-name-setname vsan vsan-id
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. Crie um conjunto de zonas de armazenamento e adicione as zonas de armazenamento ao novo conjunto.

Execute estas etapas em apenas um switch na malha.

a. Crie o conjunto de zonas de armazenamento:

```
zoneset name STOR-zone-set-name vsan vsan-id
```

b. Adicione zonas de armazenamento ao conjunto de zonas:

```
member STOR-zone-name
```

c. Ative o conjunto de zonas:

```
zoneset activate name STOR-zone-set-name vsan vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Crie zonas FCVI e adicione as portas FCVI a elas.

Cada zona FCVI contém as portas FCVI de todos os controladores de um grupo de RD.

Execute estas etapas em apenas um switch na malha.

O zoneamento depende do modelo de ponte FC-para-SAS que você está usando. Para obter detalhes, consulte a seção para sua ponte modelo. Os exemplos mostram portas de switch Brocade, então ajuste suas portas de acordo.

- "Zoneamento para pontes FibreBridge 7500N ou 7600N usando uma porta FC"
- "Zoneamento para pontes FibreBridge 7500N usando ambas as portas FC"

Cada zona de storage contém as portas do iniciador HBA de todos os controladores e uma única porta que conecta uma ponte FC a SAS.

a. Crie as zonas FCVI:

```
zone name FCVI-zone-name vsan vsanid
```

b. Adicione portas FCVI à zona:

```
member FCVI-zone-name
```

c. Ative o conjunto de zonas:

```
zoneset activate name FCVI-zone-name-set-name vsan vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

7. Crie um conjunto de zonas FCVI e adicione as zonas FCVI a ele:

   Execute estas etapas em apenas um switch na malha.

   a. Crie o conjunto de zonas FCVI:

      `zoneset name *FCVI_zone_set_name* vsan *vsan-id*`

   b. Adicione zonas FCVI ao conjunto de zonas:

      `member *FCVI_zonename*`

   c. Ative o conjunto de zonas:

      `zoneset activate name *FCVI_zone_set_name* vsan *vsan-id*`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
    ...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

8. Verifique o zoneamento:

   `show zone`

9. Repita as etapas anteriores na segunda malha de switch FC.

Garantir que a configuração do switch FC seja salva

Você deve garantir que a configuração do switch FC esteja salva na configuração de inicialização em todos os switches.

Passo

Execute o seguinte comando em ambas as malhas de switch FC:

`copy running-config startup-config`

```
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# copy running-config startup-config
```

Instalar pontes FC a SAS e gavetas de disco SAS

Você instala e faz o cabeamento de pontes ATTO FibreBridge e gavetas de disco SAS ao adicionar novo armazenamento à configuração.

Sobre esta tarefa

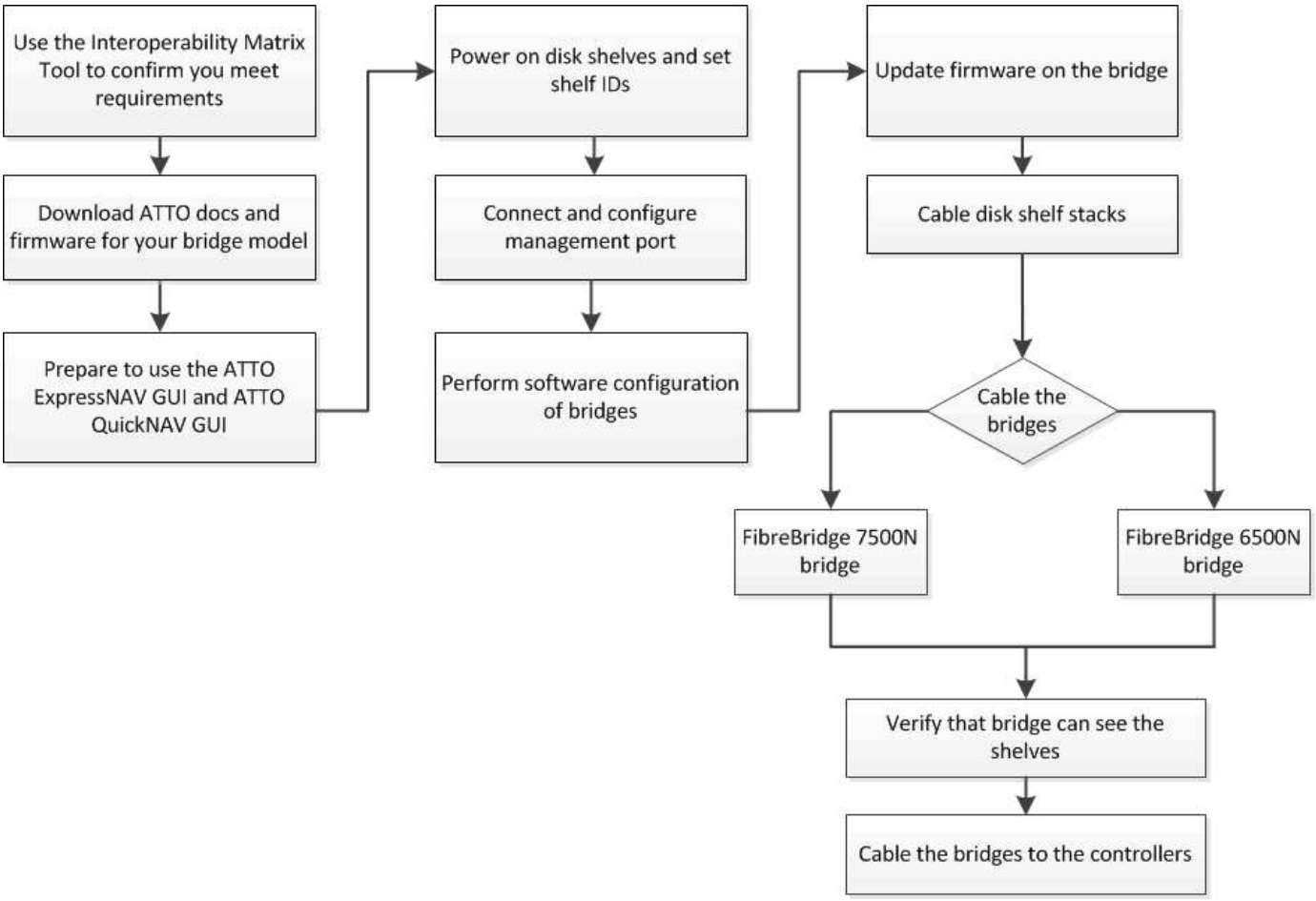
Para sistemas recebidos de fábrica, as pontes FC para SAS são pré-configuradas e não exigem configuração adicional.

Este procedimento é escrito com a suposição de que você está usando as interfaces de gerenciamento de bridge recomendadas: A GUI ATTO ExpressNAV e o utilitário ATTO Quicknav.

Você usa a GUI ATTO ExpressNAV para configurar e gerenciar uma bridge e atualizar o firmware da bridge. Você usa o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet bridge.

Em vez disso, você pode usar outras interfaces de gerenciamento, se necessário, como uma porta serial ou Telnet para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet e FTP para atualizar o firmware da ponte.

Este procedimento utiliza o seguinte fluxo de trabalho:



Gerenciamento na banda das pontes FC para SAS

Começando com o ONTAP 9.5 com o FibreBridge 7500N ou 7600N bridges, *in-band Management* das bridges é suportado como uma alternativa ao gerenciamento IP das bridges. A partir do ONTAP 9.8, o gerenciamento fora da banda está obsoleto.

A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Ao usar o gerenciamento na banda, as bridges podem ser gerenciadas e monitoradas a partir da CLI do ONTAP por meio da conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário, reduzindo a vulnerabilidade de segurança da ponte.

A disponibilidade do gerenciamento em banda das pontes depende da versão do ONTAP:

- A partir do ONTAP 9.8, as bridges são gerenciadas por meio de conexões na banda por padrão e o gerenciamento fora da banda das bridges via SNMP é obsoleto.
- ONTAP 9.5 a 9,7: O gerenciamento na banda ou o gerenciamento SNMP fora da banda é suportado.
- Antes do ONTAP 9.5, somente o gerenciamento SNMP fora da banda é suportado.

Os comandos Bridge CLI podem ser emitidos a partir do comando ONTAP interface `storage bridge run-cli -name` *`bridge_name`* `-command` *`bridge_command_name`* na interface ONTAP.

O uso do gerenciamento na banda com acesso IP desativado é recomendado para melhorar a segurança limitando a conetividade física à ponte.

Limites e regras de anexo da ponte FibreBridge 7600N e 7500N

Reveja os limites e considerações ao anexar pontes FibreBridge 7600N e 7500N.

Limites das pontes FibreBridge 7600N e 7500N

- O número máximo de unidades HDD e SSD combinadas é 240.
- O número máximo de unidades SSD é 96.
- O número máximo de SSDs por porta SAS é 48.
- O número máximo de gavetas por porta SAS é de 10.

Regras de anexo de ponte FibreBridge 7600N e 7500N

- Não misture unidades SSD e HDD na mesma porta SAS.
- Distribua as gavetas uniformemente entre as portas SAS.
- Você não deve ter DS460 gavetas na mesma porta SAS que outros tipos de gaveta (por exemplo, DS212 ou DS224 gavetas).

Exemplo de configuração

A seguir mostra um exemplo de configuração para conectar quatro gavetas DS224 com unidades SSD e seis gavetas DS224 com unidades HDD:

Porta de SAS	Compartimentos e unidades
Porta SAS A	2x DS224 gavetas com unidades SSD
Porta SAS-B	2x DS224 gavetas com unidades SSD
Porta SAS-C	3x DS224 gavetas com unidades HDD
Porta SAS-D	3x DS224 gavetas com unidades HDD

Prepare-se para a instalação

Ao se preparar para instalar as pontes como parte do novo sistema MetroCluster, você deve garantir que o sistema atenda a certos requisitos, incluindo atender aos requisitos de configuração e configuração das pontes. Outros requisitos incluem o download dos documentos necessários, o utilitário ATTO Quicknav e o firmware da ponte.

Antes de começar

- Seu sistema já deve ser instalado em um rack se ele não foi enviado em um gabinete do sistema.
- Sua configuração deve estar usando modelos de hardware e versões de software compatíveis.

  No "Ferramenta de Matriz de interoperabilidade NetApp (IMT)", você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Cada switch FC precisa ter uma porta FC disponível para que uma ponte seja conetada a ele.
- Você precisa se familiarizar com como lidar com cabos SAS e com as considerações e práticas

recomendadas para instalação e cabeamento de compartimentos de disco.

O *Installation and Service Guide* do modelo de compartimento de disco descreve as considerações e as práticas recomendadas.

- O computador que você está usando para configurar as bridges deve estar executando um navegador da Web compatível com ATTO para usar a GUI ATTO ExpressNAV.

  As Notas de versão do produto *ATTO* têm uma lista atualizada de navegadores da Web compatíveis. Você pode acessar este documento a partir do SITE DA ATTO, conforme descrito nas etapas a seguir.

Passos

1. Faça o download do *Installation and Service Guide* do modelo do compartimento de disco:
   a. Acesse o site DA ATTO usando o link fornecido para o modelo do FibreBridge e baixe o manual e o utilitário Quicknav.

      O *ATTO FibreBridge Installation and Operation Manual* para sua ponte de modelo tem mais informações sobre interfaces de gerenciamento.

      Você pode acessar este e outros conteúdos no SITE DA ATTO usando o link fornecido na página Descrição DO ATTO Fibrebridge.

2. Reúna o hardware e as informações necessárias para usar as interfaces de gerenciamento de bridge recomendadas, a GUI ATTO ExpressNAV e o utilitário ATTO Quicknav:
   a. Determine um nome de usuário e uma senha não padrão (para acessar as pontes).

      Você deve alterar o nome de usuário e a senha padrão.

   b. Se estiver configurando para gerenciamento IP das pontes, você precisará do cabo Ethernet blindado fornecido com as pontes (que se coneta da porta 1 de gerenciamento Ethernet da ponte à sua rede).
   c. Se estiver configurando para gerenciamento IP das bridges, você precisará de um endereço IP, máscara de sub-rede e informações de gateway para a porta 1 de gerenciamento Ethernet em cada bridge.
   d. Desative os clientes VPN no computador que você está usando para configuração.

      Os clientes VPN ativos fazem com que o Quicknav procure por bridges falhem.

Instalar a ponte FC para SAS e as gavetas SAS

Depois de garantir que o sistema atenda a todos os requisitos em "preparando-se para a instalação", você pode instalar seu novo sistema.

Sobre esta tarefa

- A configuração do disco e do compartimento em ambos os locais deve ser idêntica.

  Se um agregado não espelhado for usado, a configuração de disco e compartimento em cada local pode ser diferente.

  Todos os discos do grupo de recuperação de desastres devem usar o mesmo tipo de conexão e estar visíveis para todos os nós do grupo de recuperação de desastres, independentemente dos discos usados para agregado espelhado ou não espelhado.

- Os requisitos de conetividade do sistema para distâncias máximas para prateleiras de disco, switches FC e dispositivos de fita de backup usando cabos de fibra ótica multimodo de 50 mícrones, também se aplicam a pontes FibreBridge.

  "NetApp Hardware Universe"

- Uma combinação de IOM12 módulos e IOM3 módulos não é suportada na mesma pilha de storage. Uma combinação de IOM12 módulos e IOM6 módulos é compatível com a mesma pilha de storage se o sistema estiver executando uma versão compatível do ONTAP.

> O ACP na banda é compatível sem cabeamento adicional nas seguintes gavetas e ponte FibreBridge 7500N ou 7600N:
>
> - IOM12 (DS460C) atrás de uma ponte de 7500N ou 7600N com ONTAP 9.2 e posterior
> - IOM12 (DS212C e DS224C) atrás de uma ponte 7500N ou 7600N com ONTAP 9.1 e posterior

> As gavetas SAS em configurações de MetroCluster não são compatíveis com cabeamento ACP.

Ative o acesso à porta IP na ponte FibreBridge 7600N, se necessário

Se você estiver usando uma versão do ONTAP anterior a 9,5, ou de outra forma planeja usar o acesso fora da banda à ponte FibreBridge 7600N usando telnet ou outros protocolos e serviços de porta IP (FTP, ExpressNAV, ICMP ou Quicknav), você pode ativar os serviços de acesso através da porta do console.

Sobre esta tarefa

Ao contrário das pontes ATTO FibreBridge 7500N, a ponte FibreBridge 7600N é fornecida com todos os protocolos e serviços de porta IP desativados.

A partir do ONTAP 9.5, *gerenciamento na banda* das bridges é suportado. Isso significa que as pontes podem ser configuradas e monitoradas a partir da CLI do ONTAP por meio da conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário e as interfaces do usuário da ponte não são necessárias.

A partir do ONTAP 9.8, *gerenciamento na banda* das bridges é suportado por padrão e o gerenciamento SNMP fora da banda é obsoleto.

Essa tarefa é necessária se você estiver usando **não** o gerenciamento na banda para gerenciar as bridges. Neste caso, você precisa configurar a ponte através da porta de gerenciamento Ethernet.

Passos

1. Acesse a interface do console de ponte conetando um cabo serial à porta serial na ponte FibreBridge 7600N.
2. Usando o console, ative os serviços de acesso e salve a configuração:

   ```
   set closeport none

   saveconfiguration
   ```

   O `set closeport none` comando habilita todos os serviços de acesso na ponte.

3. Desative um serviço, se desejado, emitindo o `set closeport` comando e repetindo o comando conforme necessário até que todos os serviços desejados sejam desativados:

   `set closeport service`

   O `set closeport` comando desativa um único serviço de cada vez.

   O parâmetro *`service`* pode ser especificado como um dos seguintes:

   - expressarsnav
   - ftp
   - icmp
   - navegação rápida
   - snmp
   - telnet

   Pode verificar se um protocolo específico está ativado ou desativado utilizando o `get closeport` comando.

4. Se você estiver habilitando o SNMP, você também deve emitir o seguinte comando:

   `set SNMP enabled`

   SNMP é o único protocolo que requer um comando de ativação separado.

5. Guardar a configuração:

   `saveconfiguration`

Configurar as pontes FC para SAS

Antes de fazer o cabeamento do modelo das pontes FC para SAS, você deve configurar as configurações no software FibreBridge.

Antes de começar

Você deve decidir se vai usar o gerenciamento em banda das pontes.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Sobre esta tarefa

Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

Passos

1. Configure a porta do console serial no ATTO FibreBridge definindo a velocidade da porta para 115000 bauds:

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

   A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.

3. Se estiver configurando para gerenciamento IP, conete a porta 1 de gerenciamento Ethernet em cada bridge à rede usando um cabo Ethernet.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   A porta 1 de gerenciamento Ethernet permite que você baixe rapidamente o firmware da ponte (usando interfaces de gerenciamento ATTO ExpressNAV ou FTP) e recupere arquivos principais e extraia logs.

4. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual* para o modelo de bridge.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

5. Configure a ponte.

   Você deve anotar o nome de usuário e a senha que você designar.

   > Não configure a sincronização de tempo no ATTO FibreBridge 7600N ou 7500N. A sincronização de tempo para O ATTO FibreBridge 7600N ou 7500N é definida para a hora do cluster depois que a ponte é descoberta pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

   a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

Se estiver usando a CLI, você deve executar os seguintes comandos:

```
set ipaddress mp1 ip-address

set ipsubnetmask mp1 subnet-mask

set ipgateway mp1 x.x.x.x

set ipdhcp mp1 disabled

set ethernetspeed mp1 1000
```

b. Configure o nome da ponte.

As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set bridgename bridge_name
```

c. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte:

```
set SNMP enabled
```

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

6. Configurar as portas FC de ponte.

a. Configure a taxa/velocidade de dados das portas FC em ponte.

A taxa de dados FC suportada depende da ponte do modelo.

- A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
- A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.

A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pela porta FC do módulo do controlador à qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCDataRate <port-number> <port-speed>
```

b. Se você estiver configurando uma ponte FibreBridge 7500N, configure o modo de conexão que a porta usa para "ptp".

A configuração FCConnMode não é necessária ao configurar uma ponte FibreBridge 7600N.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCConnMode <port-number> ptp
```

c. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, você deve configurar ou desativar a porta FC2.

- Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.
- Se você não estiver usando a segunda porta, então você deve desativar a porta:

```
FCPortDisable <port-number>
```

O exemplo a seguir mostra a desativação da porta FC 2:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, desative as portas SAS não utilizadas:

```
SASPortDisable sas-port
```

As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas.

Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas. O exemplo a seguir mostra a desativação da porta SAS B. você deve desabilitar as portas SAS C e D da mesma forma:

```
SASPortDisable b

SAS Port B has been disabled.
```

7. Proteja o acesso à ponte e salve a configuração da ponte. Escolha uma opção abaixo, dependendo da versão do ONTAP que seu sistema está sendo executado.

Versão de ONTAP	Passos
ONTAP 9 1.5 ou posterior	a. Veja o status das pontes: `storage bridge show` A saída mostra qual ponte não está protegida. b. Fixe a ponte: `securebridge`
ONTAP 9 1.4 ou anterior	a. Veja o status das pontes: `storage bridge show` A saída mostra qual ponte não está protegida. b. Verifique o estado das portas da ponte não protegida: `info` A saída mostra o status das portas Ethernet MP1 e MP2. c. Se a porta Ethernet MP1 estiver ativada, execute: `set EthernetPort mp1 disabled` Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2. d. Salve a configuração da ponte. Você deve executar os seguintes comandos: `SaveConfiguration` `FirmwareRestart` Você é solicitado a reiniciar a ponte.

8. Depois de concluir a configuração do MetroCluster, use o `flashimages` comando para verificar sua versão do firmware do FibreBridge e, se as bridges não estiverem usando a versão mais recente suportada, atualize o firmware em todas as bridges na configuração.

   "Mantenha os componentes do MetroCluster"

Cable disk shelves to the bridges

Você precisa usar as pontes FC para SAS corretas para fazer o cabeamento das gavetas de disco.

Opções

- Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando IOM12 módulos
- Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando módulos IOM6 ou IOM3

Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando IOM12 módulos

Depois de configurar a ponte, você pode iniciar o cabeamento do seu novo sistema.

Sobre esta tarefa

Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).

Passos

1. Encadeie em série as gavetas de disco em cada pilha:

   a. Começando pela primeira gaveta lógica na stack, conecte Iom A porta 3 à IOM a porta 1 na próxima gaveta até que cada IOM A na stack seja conectada.

   b. Repita o subpasso anterior para IOM B.

   c. Repita as subetapas anteriores para cada pilha.

   O *Installation and Service Guide* do modelo de compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.

2. Ligue as gavetas de disco e, em seguida, defina as IDs de gaveta.
   - É necessário desligar cada compartimento de disco.
   - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
3. Cable disk shelves to the FibreBridge bridges.

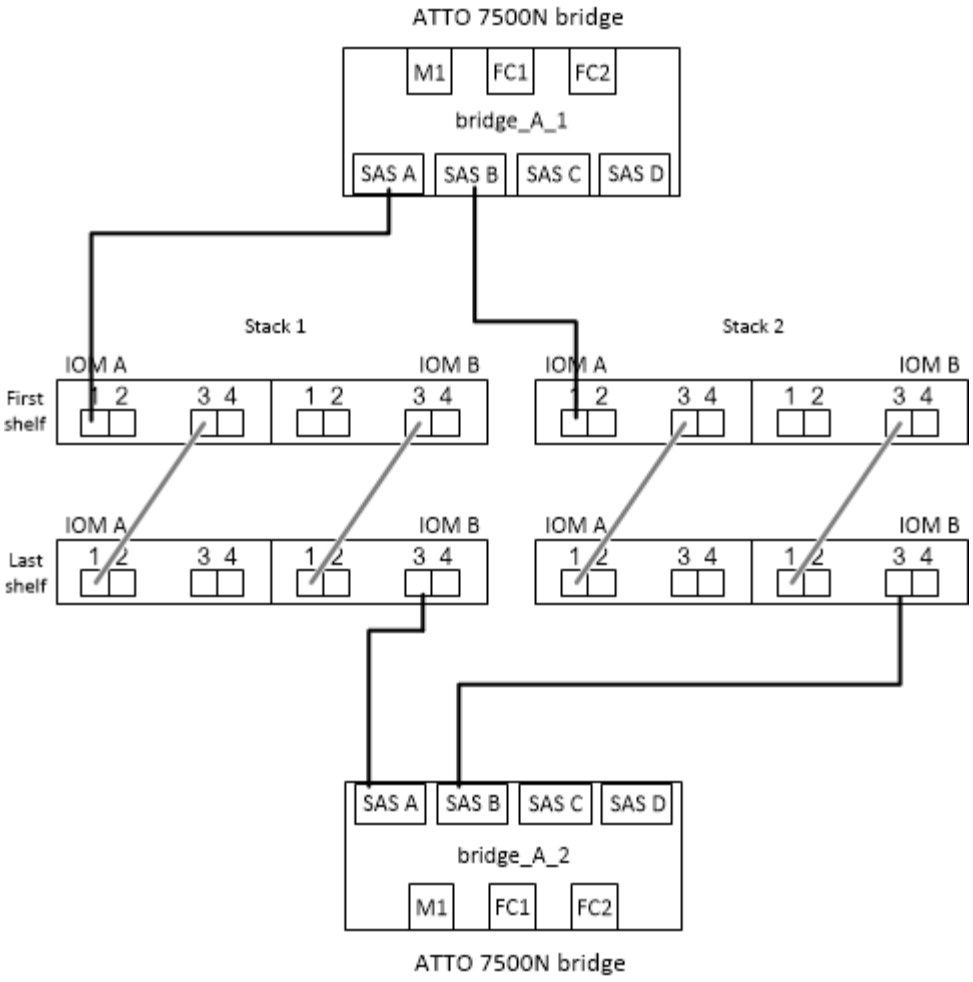
   a. Para a primeira stack de gavetas de disco, cable IOM A da primeira gaveta para a porta SAS a na FibreBridge A e cable IOM B da última gaveta para a porta SAS a na FibreBridge B.

   b. Para stacks de gaveta adicionais, repita a etapa anterior usando a próxima porta SAS disponível nas bridges do FibreBridge, usando a porta B para a segunda stack, a porta C para a terceira stack e a porta D para a quarta stack.

   c. Durante o cabeamento, conete as pilhas baseadas nos módulos IOM12 e IOM3/IOM6 à mesma ponte desde que estejam conetadas a portas SAS separadas.

      Cada stack pode usar modelos diferentes de IOM, mas todas as gavetas de disco em uma stack precisam usar o mesmo modelo.

      A ilustração a seguir mostra as prateleiras de disco conetadas a um par de pontes FibreBridge 7600N ou 7500N:



Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras usando módulos IOM6 ou IOM3

Depois de configurar a ponte, você pode iniciar o cabeamento do seu novo sistema. A ponte FibreBridge 7600N ou 7500N usa conetores mini-SAS e suporta prateleiras que usam módulos IOM6 ou IOM3.

Sobre esta tarefa

Os módulos IOM3 não são suportados com bridges FibreBridge 7600N.

Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).

Passos

1. Encadeie as prateleiras em cada pilha.

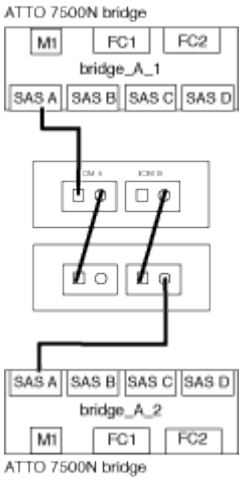
   a. Para a primeira stack de gavetas, cable IOM Uma porta quadrada da primeira gaveta para a porta SAS A na FibreBridge A.

   b. Para a primeira stack de gavetas, a porta circular IOM B do cabo da última gaveta até a porta SAS A no FibreBridge B.

   O *Installation and Service Guide* para o modelo de prateleira fornece informações detalhadas sobre prateleiras de encadeamento em série.

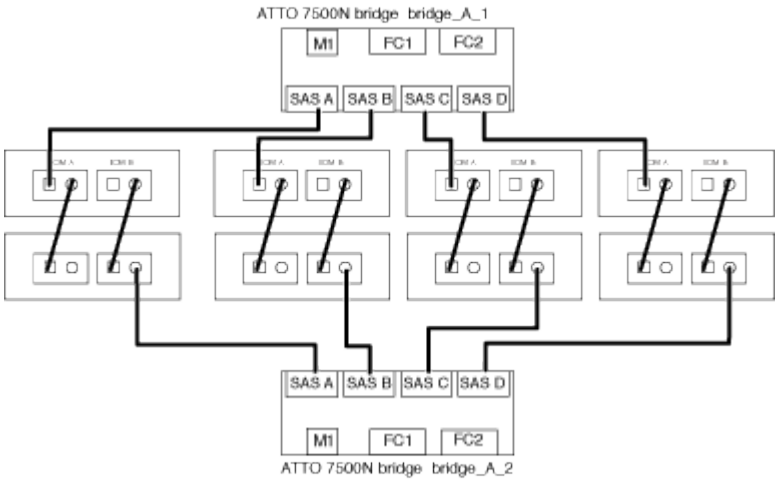
   "Guia de instalação e serviço das gavetas de disco SAS para DS4243, DS2246, DS4486 e DS4246"

A ilustração a seguir mostra um conjunto de pontes cabeadas para uma pilha de prateleiras:



2. Para stacks de gaveta adicionais, repita as etapas anteriores usando a próxima porta SAS disponível nas bridges do FibreBridge, usando a porta B para uma segunda stack, a porta C para uma terceira stack e a porta D para uma quarta stack.

   A ilustração a seguir mostra quatro pilhas conetadas a um par de pontes FibreBridge 7600N ou 7500N.



Verifique a conectividade da ponte e o cabeamento das portas FC da ponte

Você deve verificar se cada bridge pode detetar todas as unidades de disco e, em seguida, fazer o cabeamento de cada bridge para os switches FC locais.

Passos

1. Verifique se cada bridge pode detetar todas as unidades de disco e prateleiras de disco às quais está conetada:

Se você estiver usando o…	Então…

ATTO ExpressNAV GUI	a. Em um navegador da Web compatível, insira o endereço IP de uma ponte na caixa do navegador. Você é levado para a página inicial DO ATTO FibreBridge da ponte para a qual você inseriu o endereço IP, que tem um link. b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte. A página de status ATTO FibreBridge da ponte é exibida com um menu à esquerda. c. Clique em **Avançado**. d. Visualize os dispositivos conetados usando o comando sastargets e clique em **Submit**.
Conexão de porta serial	Ver os dispositivos ligados: `sastargets`

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos. Por exemplo, a saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

Se o texto "Esponse truncado" aparecer no início da saída, você pode usar o Telnet para conetar-se à ponte e digitar o mesmo comando para ver toda a saída.

2. Verifique se a saída do comando mostra que a ponte está conetada a todos os discos e compartimentos de disco na pilha à qual deve ser conetada.

Se a saída for…	Então…
Correto	Repita Passo 1 para cada ponte restante.

Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo o cabeamento. Cable disk shelves to the bridges b. Repita Passo 1.

3. Faça o cabeamento de cada ponte aos switches FC locais, usando o cabeamento da tabela para sua configuração e modelo de switch e o modelo de ponte FC para SAS:

   A segunda conexão de porta FC na ponte FibreBridge 7500N não deve ser cabeada até que o zoneamento seja concluído.

   Consulte as atribuições de portas da sua versão do ONTAP.

4. Repita o passo anterior nas pontes no local do parceiro.

Informações relacionadas

Você precisa verificar se está usando as atribuições de portas especificadas quando você faz o cabeamento dos switches FC ao usar o ONTAP 9.1 e posterior.

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Proteja ou desprenda a ponte FibreBridge

Para desativar facilmente protocolos Ethernet potencialmente inseguros em uma ponte, começando com o ONTAP 9.5, você pode proteger a ponte. Isto desativa as portas Ethernet da ponte. Você também pode reativar o acesso Ethernet.

Sobre esta tarefa

- A proteção da ponte desativa os protocolos e serviços de porta telnet e de outras portas IP (FTP, ExpressNAV, ICMP ou Quicknav) na ponte.
- Este procedimento usa gerenciamento fora da banda usando o prompt ONTAP, que está disponível a partir do ONTAP 9.5.

  Você pode emitir os comandos da CLI de bridge se não estiver usando o gerenciamento fora da banda.

- O `unsecurebridge` comando pode ser usado para reativar as portas Ethernet.
- No ONTAP 9.7 e anteriores, executar o `securebridge` comando no FibreBridge ATTO pode não atualizar o status da ponte corretamente no cluster de parceiros. Se isso ocorrer, execute o `securebridge` comando do cluster de parceiros.

A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. A partir do prompt ONTAP do cluster que contém a ponte, proteja ou desprenda a ponte.
   - O seguinte comando protege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
```

- O comando a seguir desprotege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. No prompt ONTAP do cluster que contém a ponte, salve a configuração da ponte:

   `storage bridge run-cli -bridge *bridge-name* -command saveconfiguration`

   O seguinte comando protege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
saveconfiguration
```

3. No prompt ONTAP do cluster que contém a ponte, reinicie o firmware da ponte:

   `storage bridge run-cli -bridge *bridge-name* -command firmwarerestart`

   O seguinte comando protege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```

Configurar o hardware para compartilhar uma malha Brocade 6510 FC durante a transição

Configuração de hardware para compartilhamento de uma malha Brocade 6510 FC durante a transição

Se a configuração do MetroCluster de malha de 7 modos usar os switches Brocade 6510, você poderá compartilhar as malhas de switches existentes com a nova configuração do Clustered MetroCluster. Malha de switch compartilhada significa que a nova configuração do MetroCluster não exige uma nova malha de switch separada. Esta configuração temporária só é suportada com o switch Brocade 6510 para fins de transição.

Antes de começar

- O MetroCluster de malha de 7 modos deve estar usando os switches Brocade 6510.

  Se a configuração do MetroCluster não estiver usando os switches Brocade 6510, os switches devem ser atualizados para o Brocade 6510 antes de usar este procedimento.

- A configuração de MetroCluster de malha de 7 modos deve estar usando apenas gavetas de storage SAS.

  Se a configuração existente incluir compartimentos de storage FC (como FC DS14mk4), o compartilhamento de malha do switch FC não será compatível.

- Os SFPs nas portas do switch usados pela nova configuração do MetroCluster em cluster devem suportar taxas de 16 Gbps.

  O MetroCluster de malha de 7 modos existente pode permanecer conetado a portas usando SFPs de 8

Gbps ou 16 Gbps.

- Em cada um dos quatro switches Brocade 6510, as portas 24 a 45 devem estar disponíveis para conetar as portas dos novos componentes do MetroCluster.
- Você deve verificar se os ISLs existentes estão nas portas 46 e 47.
- Os switches Brocade 6510 devem estar executando uma versão de firmware FOS compatível com o 7-Mode Fabric MetroCluster e a configuração Clustered ONTAP MetroCluster.

Depois de terminar

Depois de compartilhar a malha e concluir a configuração do MetroCluster, você pode migrar dados da configuração do MetroCluster de malha de 7 modos.

Após a transição dos dados, você poderá remover o cabeamento MetroCluster de malha de 7 modos e, se desejar, mover o cabeamento ONTAP MetroCluster em cluster para as portas de número inferior usadas anteriormente para o cabeamento MetroCluster de 7 modos. As portas são mostradas na seção "Revisão de atribuições de portas de switch FC para um MetroCluster de quatro nós". Você deve ajustar o zoneamento para as portas reorganizadas.

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Informações relacionadas

"Transição baseada em cópia"

Revisão dos requisitos de licença do Brocade

Você precisa de certas licenças para os switches em uma configuração do MetroCluster. Você deve instalar essas licenças em todos os quatro switches.

A configuração do MetroCluster tem os seguintes requisitos de licença do Brocade:

- Licença de entroncamento para sistemas que utilizam mais de um ISL, conforme recomendado.
- Licença alargada de tecido (para distâncias ISL superiores a 6 km)
- Licença Enterprise para locais com mais de um ISL e uma distância ISL superior a 6 km

  A licença Enterprise inclui o consultor de rede Brocade e todas as licenças, exceto para licenças de porta adicionais.

Você pode verificar se as licenças estão instaladas usando o comando 'license'.

Para o Fabric os 8,2.x e anteriores

Executar o comando `licenseshow`.

Para o Fabric os 9,0 e posterior

Executar o comando `license --show`.

Se você não tiver essas licenças, entre em Contato com seu representante de vendas antes de prosseguir.

Colocar em pilha os componentes de hardware

Se você não recebeu o equipamento já instalado em armários, você deve colocar os componentes em rack.

Sobre esta tarefa

Esta tarefa tem de ser executada em ambos os sites da MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   O espaço em rack depende do modelo de plataforma dos módulos do controlador, dos tipos de switch e do número de pilhas de compartimento de disco na sua configuração.

2. Aterre-se corretamente.
3. Instale os módulos do controlador no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Instale os switches FC no rack ou gabinete.
5. Instale as gavetas de disco, ligue-as e, em seguida, defina as IDs das gaveta.
   - É necessário desligar cada compartimento de disco.
   - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
6. Instalar cada ponte FC para SAS:

   a. Fixe os suportes "L" na parte frontal da ponte à frente do rack (montagem embutida) com os quatro parafusos.

      As aberturas nos suportes da ponte "L" estão em conformidade com o padrão de rack ETA-310-X para racks de 19 polegadas (482,6 mm).

      O *ATTO FibreBridge Installation and Operation Manual* do seu modelo de ponte contém mais informações e uma ilustração da instalação.

      > Para um acesso adequado ao espaço da porta e manutenção da FRU, você deve deixar espaço 1UD abaixo do par de pontes e cobrir esse espaço com um painel de supressão sem ferramentas.

   b. Conete cada ponte a uma fonte de alimentação que forneça um aterramento adequado.
   c. Ligue cada ponte.

      > Para obter a resiliência máxima, as bridges que estão conectadas à mesma stack de shelves de disco devem ser conectadas a diferentes fontes de energia.

   O LED bridge Ready pode demorar até 30 segundos a acender, indicando que a ponte concluiu a sequência de autoteste de ativação.

Fazer o cabeamento das novas controladoras MetroCluster às malhas FC existentes

Em cada controladora na configuração de cluster ONTAP MetroCluster, o adaptador FC-VI e HBAs devem ser cabeados para portas específicas nos switches FC existentes.

Passos

1. Faça o cabeamento das portas FC-VI e HBA de acordo com a seguinte tabela:

Local A		Local B	
Conetar este Site Um componente e uma porta…	Porta FC_switch_A_1…	Ligar este componente do local B e porta…	Porta FC_switch_B_1…
Controller_A_1 FC-VI porta 1	32	Controller_B_1 FC-VI porta 1	32
Controller_A_1 HBA porta 1	33	Controlador_B_1 porta HBA 1	33
Controller_A_1 HBA porta 2	34	Controlador_B_1 porta HBA 2	34
Controller_A_2 FC-VI porta 1	35	Controller_B_2 FC-VI porta 1	35
controller_A_2 HBA 1	36	controller_B_2 HBA 1	36
controller_A_2 HBA 2	37	controller_B_2 HBA 2	37

2. Cable cada ponte FC-SAS na primeira malha de switch aos switches FC.

   O número de bridges varia dependendo do número de stacks de armazenamento SAS.

Local A		Local B	
Este local É Uma ponte…	Porta FC_switch_A_1…	Cable this Site B bridge…	Porta FC_switch_B_1…
bridge_A_1_38	38	bridge_B_1_38	38
bridge_A_1_39	39	bridge_B_1_39	39

3. Conete cada ponte na segunda malha de switch aos switches FC.

   O número de bridges varia dependendo do número de stacks de armazenamento SAS.

Local A	Local B

Este local É Uma ponte…	Porta FC_switch_A_2…	Cable this Site B bridge…	Porta FC_switch_B_2…
bridge_A_2_38	38	bridge_B_2_38	38
bridge_A_2_39	39	bridge_B_2_39	39

Configure o compartilhamento de malhas de switch entre o modo 7 e a configuração do MetroCluster em cluster

Desativação de uma das malhas de comutação

Você deve desativar uma das malhas do switch para que possa modificar sua configuração. Depois de concluir a configuração e reativar a malha do switch, você repetirá o processo na outra malha.

Antes de começar

Você deve ter executado o utilitário fmc_dc na configuração existente do 7-Mode Fabric MetroCluster e resolvido quaisquer problemas antes de iniciar o processo de configuração.

Sobre esta tarefa

Para garantir a operação contínua da configuração do MetroCluster, não é necessário desativar a segunda malha enquanto a primeira malha estiver desativada.

Passos

1. Desative cada um dos switches na estrutura:

   `switchCfgPersistentDisable`

   Se este comando não estiver disponível, use o `switchDisable` comando.

   - O exemplo a seguir mostra o comando emitido em FC_switch_A_1:

     ```
     FC_switch_A_1:admin> switchCfgPersistentDisable
     ```

   - O exemplo a seguir mostra o comando emitido em FC_switch_B_1:

     ```
     FC_switch_B_1:admin> switchCfgPersistentDisable
     ```

2. Certifique-se de que a configuração do MetroCluster de 7 modos esteja funcionando corretamente usando a estrutura redundante:

   a. Confirme se o failover de controladora está em bom estado
   `cf status`

```
node_A> cf status
Controller Failover enabled, node_A is up.
VIA Interconnect is up (link 0 down, link 1 up).
```

b. Confirme se os discos estão visíveis
`storage show disk -p`

```
node_A> storage show disk -p

PRIMARY                    PORT  SECONDARY          PORT SHELF BAY
-------------------------- ----  ------------------ ---- ---------
Brocade-6510-2K0GG:5.126L27  B                           1    0
Brocade-6510-2K0GG:5.126L28  B                           1    1
Brocade-6510-2K0GG:5.126L29  B                           1    2
Brocade-6510-2K0GG:5.126L30  B                           1    3
Brocade-6510-2K0GG:5.126L31  B                           1    4

.
.
.
```

c. Confirme que os agregados estão saudáveis
`aggr status`

```
node_A> aggr status
           Aggr State           Status              Options
          aggr0 online          raid_dp, aggr       root, nosnap=on
                                mirrored
                                64-bit
```

Eliminar o zoneamento do TI e configurar as definições do IOD

Você deve excluir o zoneamento de TI existente e reconfigurar as configurações de entrega de pedidos (IOD) na malha do switch.

Passos

1. Identifique as zonas de TI configuradas na malha:

   `zone --show`

   O exemplo a seguir mostra a zona FCVI_TI_FAB_2.

```
Brocade-6510:admin> zone --show
   Defined TI zone configuration:
   TI Zone Name:   FCVI_TI_FAB_2
   Port List:      1,0; 1,3; 2,0; 2,3
   configured Status: Activated / Failover-Disabled
   Enabled Status: Activated / Failover-Disabled
```

2. Eliminar as zonas TI:

   `zone --delete zone-name`

   O exemplo a seguir mostra a exclusão da zona FCVI_TI_FAB_2.

```
Brocade-6510:admin> zone --delete FCVI_TI_FAB_2
```

3. Confirme se as zonas foram eliminadas:

   `zone --show`

   A saída deve ser semelhante ao seguinte:

```
Brocade-6510:admin> zone --show

    Defined TI zone configuration:
    no TI zone configuration defined
```

4. Guardar a configuração:

   `cfgsave`

5. Ativar entrega na encomenda:

   `iodset`

6. Selecione a política Advanced Performance Tuning (APT) 1, a Política de Roteamento baseado em portas:

   `aptpolicy 1`

7. Desativar a partilha de carga dinâmica (DLS):

   `dlsreset`

8. Verifique as configurações IOD:

   `iodshow`

   `aptpolicy`

`dlsshow`

A saída deve ser semelhante ao seguinte:

```
Brocade-6510:admin> iodshow

IOD is set

Brocade-6510:admin> aptpolicy
 Current Policy: 1

 3 : Default Policy
 1: Port Based Routing Policy
 2: Device Based Routing Policy (FICON support only)
 3: Exchange Based Routing Policy
Brocade-6510:admin> dlsshow

DLS is not set
```

Garantir que os ISLs estejam no mesmo grupo de portas e configurando o zoneamento

Você deve se certificar de que os ISLs (Inter-Switch Links) estão no mesmo grupo de portas e configurar o zoneamento para as configurações do MetroCluster para compartilhar com êxito as malhas do switch.

Passos

1. Se os ISLs não estiverem no mesmo grupo de portas, mova uma das portas ISL para o mesmo grupo de portas do outro.

   Você pode usar qualquer porta disponível, exceto 32 até 45, que são usadas pela nova configuração do MetroCluster. As portas ISL recomendadas são 46 e 47.

2. Siga as etapas na "Configuração de zoneamento em switches Brocade FC" seção para ativar o entroncamento e a zona de QoS.

   Os números de porta ao compartilhar tecidos são diferentes dos mostrados na seção. Ao compartilhar, use as portas 46 e 47 para as portas ISL. Se você moveu suas portas ISL, você precisará usar o procedimento na "Configurando as portas e (portas ISL) em um switch Brocade FC" seção para configurar as portas.

3. siga as etapas na "Configurando as portas não-e no switch Brocade" seção para configurar as portas não E.
4. Não exclua as zonas ou conjuntos de zonas que já existem nos switches backend (para o MetroCluster de malha de 7 modos), exceto as zonas de isolamento de tráfego (TI) em Passo 3.
5. Siga as etapas na "Configurando as portas e (portas ISL) em um switch Brocade FC" seção para adicionar as zonas exigidas pelo novo MetroCluster aos conjuntos de zonas existentes.

   O exemplo a seguir mostra os comandos e a saída do sistema para criar as zonas:

```
Brocade-6510-2K0GG:admin> zonecreate "QOSH2_FCVI_1", "2,32; 2,35; 1,32;
1,35"

Brocade-6510-2K0GG:admin> zonecreate "STOR_A_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 1,47"

Brocade-6510-2K0GG:admin> zonecreate "STOR_B_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 2,47"


Brocade-6510-2K0GG:admin> cfgadd config_1_FAB2, "QOSH2_FCVI_1;
STOR_A_2_47; STOR_B_2_47"

Brocade-6510-2K0GG:admin> cfgenable "config_1_FAB2"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'config_1_FAB2' configuration  (yes, y, no, n):
[no] yes

Brocade-6510-2K0GG:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only?  (yes, y, no,
n): [no] yes
Nothing changed: nothing to save, returning ...
Brocade-6510-2K0GG:admin>
```

Reativação da malha do switch e verificação da operação

Você deve habilitar a malha de switch FC e garantir que os switches e dispositivos estejam funcionando corretamente.

Passos

1. Ativar os interrutores:

   `switchCfgPersistentEnable`

   Se este comando não estiver disponível, o switch deve estar no estado habilitado após o `fastBoot` comando ser emitido.

   - O exemplo a seguir mostra o comando emitido em FC_switch_A_1:

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

- O exemplo a seguir mostra o comando emitido em FC_switch_B_1:

```
FC_switch_B_1:admin> switchCfgPersistentEnable
```

2. Verifique se os switches estão on-line e todos os dispositivos estão conetados corretamente:

   `switchShow`

   O exemplo a seguir mostra o comando emitido em FC_switch_A_1:

```
FC_switch_A_1:admin> switchShow
```

   O exemplo a seguir mostra o comando emitido em FC_switch_B_1:

```
FC_switch_B_1:admin> switchShow
```

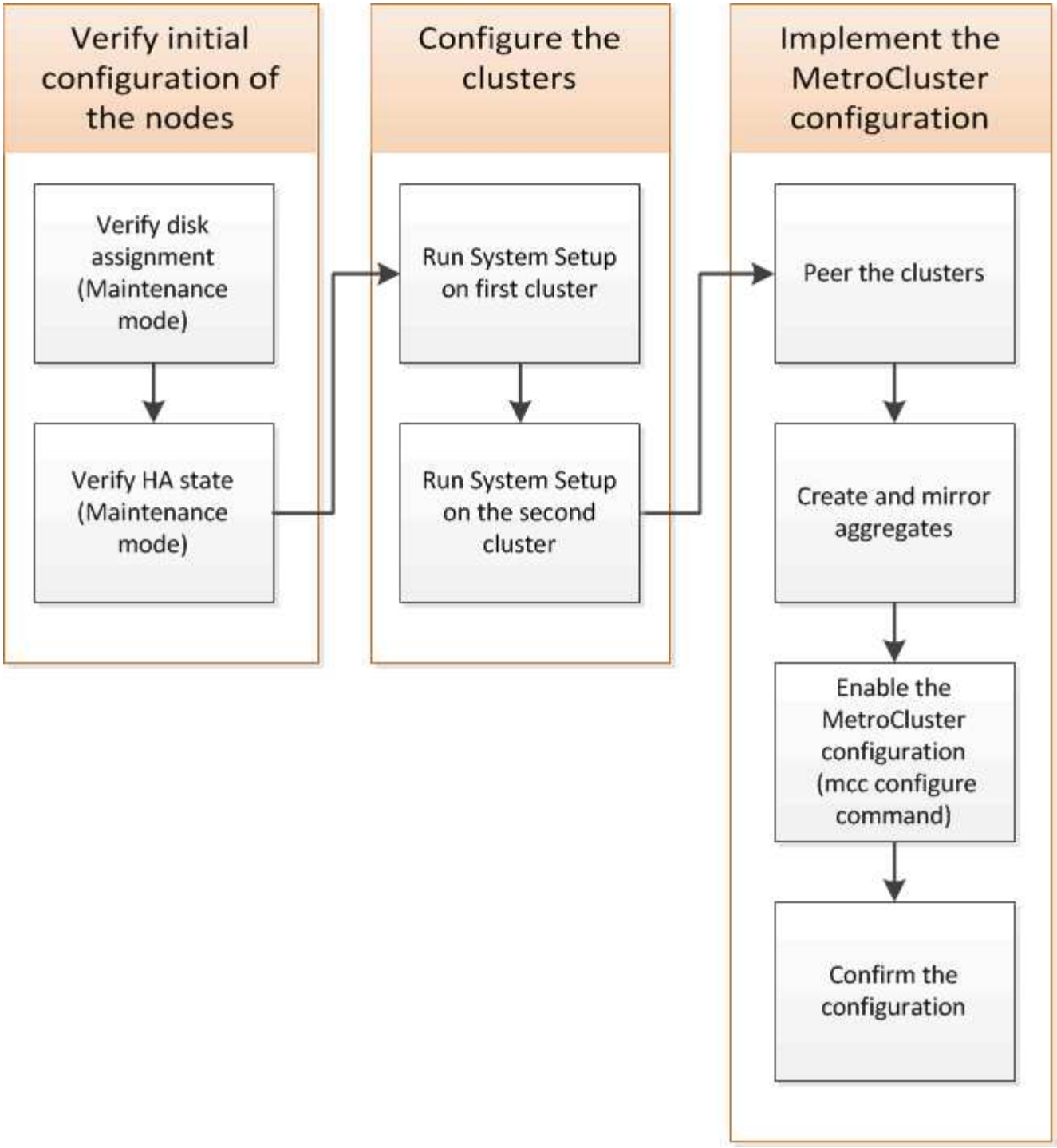
3. Execute o utilitário fmc_dc para garantir que o 7-Mode Fabric MetroCluster esteja funcionando corretamente.

   Você pode ignorar erros relacionados ao zoneamento e entroncamento de isolamento de tráfego (TI).

4. Repita as tarefas para a segunda malha do switch.

Configurando o software MetroCluster no ONTAP

É necessário configurar cada nó na configuração do MetroCluster no ONTAP, incluindo as configurações no nível do nó e a configuração dos nós em dois locais. Você também deve implementar a relação MetroCluster entre os dois sites. As etapas para sistemas com compartimentos de disco nativos são ligeiramente diferentes das de sistemas com LUNs de array.



Recolha de informações necessárias

Você precisa reunir os endereços IP necessários para os módulos do controlador antes de iniciar o processo de configuração.

Folha de cálculo de informações de rede IP para o local A

Você deve obter endereços IP e outras informações de rede para o primeiro site do MetroCluster (site A) do administrador da rede antes de configurar o sistema.

Informações do switch local A (clusters comutados)

Quando você faz o cabo do sistema, você precisa de um nome de host e endereço IP de gerenciamento para cada switch de cluster. Essas informações não são necessárias se você estiver usando um cluster sem switch de dois nós ou tiver uma configuração de MetroCluster de dois nós (um nó em cada local).

Interrutor do cluster	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Interconexão 1				
Interconexão 2				
Gestão 1				
Gestão 2				

Site Um cluster de criação de informações

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster Exemplo usado neste guia: Site_A	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do site A.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1 Exemplo usado neste guia: Controller_A_1				

Nó 2 Não é necessário se estiver usando a configuração MetroCluster de dois nós (um nó em cada local). Exemplo usado neste guia: Controller_A_2				

Crie um site LIFs e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				
Nó 1 IC LIF 2				
Nó 2 IC LIF 1 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).				
Nó 2 IC LIF 2 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).				

Site A informações do servidor de tempo

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local A Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		Anfitriões de correio
Endereços IP ou nomes		Protocolo de transporte
HTTP, HTTPS OU SMTP		Servidor proxy
	Endereços de e-mail do destinatário ou listas de distribuição	Mensagens completas
	Mensagens concisas	

Local A Informação SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção, o que requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1			
Nó 2 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).			

Folha de cálculo de informações de rede IP para o local B.

Você deve obter endereços IP e outras informações de rede para o segundo site da MetroCluster (site B) do administrador da rede antes de configurar o sistema.

Informações do switch local B (clusters comutados)

Quando você faz o cabo do sistema, você precisa de um nome de host e endereço IP de gerenciamento para cada switch de cluster. Essas informações não são necessárias se você estiver usando um cluster sem switch de dois nós ou se você tiver uma configuração de MetroCluster de dois nós (um nó em cada local).

Interrutor do cluster	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Interconexão 1				
Interconexão 2				

Gestão 1				
Gestão 2				

Informações sobre a criação do cluster do local B.

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster Exemplo usado neste guia: Site_B	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do local B.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1 Exemplo usado neste guia: Controller_B_1				
Nó 2 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local). Exemplo usado neste guia: Controller_B_2				

LIFs do local B e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				
Nó 1 IC LIF 2				
Nó 2 IC LIF 1 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).				
Nó 2 IC LIF 2 Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).				

Informações do servidor de hora local B.

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local B Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		
Anfitriões de correio	Endereços IP ou nomes	
Protocolo de transporte	HTTP, HTTPS OU SMTP	

Servidor proxy		Endereços de e-mail do destinatário ou listas de distribuição
Mensagens completas		Mensagens concisas
	Parceiros	

Local B Informação SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção, o que requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1 (controlador_B_1)			
Nó 2 (controlador_B_2) Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local).			

Semelhanças e diferenças entre configurações padrão de cluster e MetroCluster

A configuração dos nós em cada cluster em uma configuração MetroCluster é semelhante à dos nós em um cluster padrão.

A configuração do MetroCluster é baseada em dois clusters padrão. Fisicamente, a configuração deve ser simétrica, com cada nó tendo a mesma configuração de hardware e todos os componentes do MetroCluster devem ser cabeados e configurados. No entanto, a configuração básica de software para nós em uma configuração MetroCluster é a mesma para nós em um cluster padrão.

Etapa de configuração	Configuração padrão de cluster	Configuração do MetroCluster
Configurar LIFs de gerenciamento, cluster e dados em cada nó.	O mesmo em ambos os tipos de clusters	
Configure o agregado raiz.	O mesmo em ambos os tipos de clusters	
Configurar nós no cluster como pares de HA	O mesmo em ambos os tipos de clusters	
Configure o cluster em um nó no cluster.	O mesmo em ambos os tipos de clusters	
Junte o outro nó ao cluster.	O mesmo em ambos os tipos de clusters	
Crie um agregado de raiz espelhado.	Opcional	Obrigatório

Espreite os clusters.	Opcional	Obrigatório
Ative a configuração do MetroCluster.	Não se aplica	Obrigatório

Verificar e configurar o estado HA dos componentes no modo Manutenção

Ao configurar um sistema de storage em uma configuração MetroCluster FC, você deve garantir que o estado de alta disponibilidade (HA) dos componentes do chassi e do módulo da controladora seja mcc ou mcc-2n para que esses componentes sejam inicializados corretamente. Embora esse valor deva ser pré-configurado em sistemas recebidos de fábrica, você ainda deve verificar a configuração antes de continuar.

Se o estado HA do módulo do controlador e do chassis estiver incorreto, não poderá configurar o MetroCluster sem reiniciar o nó. Deve corrigir a definição utilizando este procedimento e, em seguida, inicializar o sistema utilizando um dos seguintes procedimentos:

- Em uma configuração IP do MetroCluster, siga as etapas em "Restaure os padrões do sistema em um módulo do controlador".
- Em uma configuração MetroCluster FC, siga as etapas em "Restaure os padrões do sistema e configurando o tipo HBA em um módulo do controlador".

Antes de começar

Verifique se o sistema está no modo Manutenção.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado de HA correto depende da configuração do MetroCluster.

Tipo de configuração MetroCluster	Estado HA para todos os componentes…
Configuração de FC MetroCluster de oito ou quatro nós	mcc
Configuração de FC MetroCluster de dois nós	mcc-2n
Configuração IP MetroCluster de oito ou quatro nós	mccip

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA correto para a sua configuração no módulo do controlador:

Tipo de configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify controller mcc`

Configuração de FC MetroCluster de dois nós	`ha-config modify controller mcc-2n`
Configuração IP MetroCluster de oito ou quatro nós	`ha-config modify controller mccip`

3. Se o estado do sistema apresentado do chassis não estiver correto, defina o estado HA correto para a sua configuração no chassis:

Tipo de configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify chassis mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify chassis mcc-2n`
Configuração IP MetroCluster de oito ou quatro nós	`ha-config modify chassis mccip`

4. Inicialize o nó no ONTAP:

   `boot_ontap`

5. Repita todo esse procedimento para verificar o estado de HA em cada nó na configuração do MetroCluster.

Restaurando os padrões do sistema e configurando o tipo HBA em um módulo do controlador

Sobre esta tarefa

Para garantir uma instalação bem-sucedida do MetroCluster, redefina e restaure padrões nos módulos do controlador.

Importante

Essa tarefa só é necessária para configurações Stretch usando bridges FC-para-SAS.

Passos

1. No prompt Loader, retorne as variáveis ambientais à configuração padrão:

   `set-defaults`

2. Inicialize o nó no modo Manutenção e, em seguida, configure as configurações para quaisquer HBAs no sistema:

   a. Arranque no modo de manutenção:

      `boot_ontap maint`

   b. Verifique as definições atuais das portas:

      `ucadmin show`

c. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator adapter_name`
CNA Ethernet	`ucadmin modify -mode cna adapter_name`
Destino de FC	`fcadmin config -t target adapter_name`
Iniciador FC	`fcadmin config -t initiator adapter_name`

3. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

4. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

5. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

6. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

7. Inicialize o nó no menu de inicialização:

   `boot_ontap menu`

   Depois de executar o comando, aguarde até que o menu de inicialização seja exibido.

8. Limpe a configuração do nó digitando "wipeconfig" no prompt do menu de inicialização e pressione Enter.

   A tela a seguir mostra o prompt do menu de inicialização:

```
Please choose one of the following:

     (1) Normal Boot.
     (2) Boot without /etc/rc.
     (3) Change password.
     (4) Clean configuration and initialize all disks.
     (5) Maintenance mode boot.
     (6) Update flash from backup config.
     (7) Install new software first.
     (8) Reboot node.
     (9) Configure Advanced Drive Partitioning.
     Selection (1-9)?  wipeconfig
 This option deletes critical system configuration, including cluster
membership.
 Warning: do not run this option on a HA node that has been taken over.
 Are you sure you want to continue?: yes
 Rebooting to finish wipeconfig request.
```

Configurando portas FC-VI em uma placa quad-port X1132A-R6 em sistemas FAS8020

Se você estiver usando a placa quad-port X1132A-R6 em um sistema FAS8020, você pode entrar no modo de manutenção para configurar as portas 1a e 1b para uso de FC-VI e iniciador. Isso não é necessário nos sistemas MetroCluster recebidos de fábrica, nos quais as portas são definidas adequadamente para sua configuração.

Sobre esta tarefa

Esta tarefa deve ser executada no modo Manutenção.

> A conversão de uma porta FC para uma porta FC-VI com o comando uadministrador só é compatível com os sistemas FAS8020 e AFF 8020. A conversão de portas FC para portas FCVI não é compatível em nenhuma outra plataforma.

Passos

1. Desative as portas:

   ```
   storage disable adapter 1a

   storage disable adapter 1b
   ```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Verifique se as portas estão desativadas:

   `ucadmin show`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. Defina as portas a e b para o modo FC-VI:

   `ucadmin modify -adapter 1a -type fcvi`

   O comando define o modo em ambas as portas no par de portas, 1a e 1b (mesmo que apenas 1a seja especificado no comando).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. Confirme se a alteração está pendente:

```
ucadmin show
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Desligue o controlador e reinicie-o no modo de manutenção.
6. Confirme a alteração de configuração:

```
ucadmin show local
```

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

Verificando a atribuição de discos no modo Manutenção em uma configuração de oito nós ou quatro nós

Antes de iniciar totalmente o sistema no ONTAP, você pode opcionalmente inicializar no modo Manutenção e verificar a atribuição de disco nos nós. Os discos devem ser atribuídos para criar uma configuração ativo-ativo totalmente simétrica, onde cada pool tem um número igual de discos atribuídos a eles.

Sobre esta tarefa

Os novos sistemas MetroCluster têm atribuição de disco concluída antes do envio.

A tabela a seguir mostra exemplos de atribuições de pool para uma configuração do MetroCluster. Os discos são atribuídos a pools por compartimento.

Prateleiras de disco no local A

Compartimento de disco (sample_shelf_name)…	Pertence a…	E é atribuído a esse nó…
Compartimento de disco 1 (shelf_A_1_1)	Nó A 1	Piscina 0
Compartimento de disco 2 (shelf_A_1_3)		
Compartimento de disco 3 (gaveta_B_1_1)	Nó B 1	Piscina 1
Compartimento de disco 4 (gaveta_B_1_3)		
Compartimento de disco 5 (shelf_A_2_1)	Nó A 2	Piscina 0
Compartimento de disco 6 (shelf_A_2_3)		
Compartimento de disco 7 (gaveta_B_2_1)	Nó B 2	Piscina 1
Compartimento de disco 8 (gaveta_B_2_3)		
Compartimento de disco 1 (shelf_A_3_1)	Nó A 3	Piscina 0
Compartimento de disco 2 (shelf_A_3_3)		
Compartimento de disco 3 (gaveta_B_3_1)	Nó B 3	Piscina 1
Compartimento de disco 4 (gaveta_B_3_3)		
Compartimento de disco 5 (shelf_A_4_1)	Nó A 4	Piscina 0
Compartimento de disco 6 (shelf_A_4_3)		
Compartimento de disco 7 (gaveta_B_4_1)	Nó B 4	Piscina 1
Compartimento de disco 8 (gaveta_B_4_3)		

Prateleiras de disco no local B

Compartimento de disco (sample_shelf_name)…	Pertence a…	E é atribuído a esse nó…
Compartimento de disco 9 (gaveta_B_1_2)	Nó B 1	Piscina 0

Compartimento de disco 10 (gaveta_B_1_4)	Compartimento de disco 11 (shelf_A_1_2)	Nó A 1
Piscina 1	Compartimento de disco 12 (shelf_A_1_4)	Compartimento de disco 13 (gaveta_B_2_2)
Nó B 2	Piscina 0	Compartimento de disco 14 (gaveta_B_2_4)
Compartimento de disco 15 (shelf_A_2_2)	Nó A 2	Piscina 1
Compartimento de disco 16 (shelf_A_2_4)	Compartimento de disco 1 (gaveta_B_3_2)	Nó A 3
Piscina 0	Compartimento de disco 2 (gaveta_B_3_4)	Compartimento de disco 3 (shelf_A_3_2)
Nó B 3	Piscina 1	Compartimento de disco 4 (shelf_A_3_4)
Compartimento de disco 5 (gaveta_B_4_2)	Nó A 4	Piscina 0
Compartimento de disco 6 (gaveta_B_4_4)	Compartimento de disco 7 (shelf_A_4_2)	Nó B 4

Passos

1. Confirme as atribuições do compartimento:

   `disk show -v`

2. Se necessário, atribua explicitamente discos nas gavetas de disco conetadas ao pool apropriado:

   `disk assign`

   O uso de curingas no comando permite atribuir todos os discos em um compartimento de disco com um único comando. É possível identificar as IDs e os compartimentos do compartimento de disco para cada disco com o `storage show disk -x` comando.

Atribuição de propriedade de disco em sistemas que não sejam AFF

Se os nós do MetroCluster não tiverem os discos corretamente atribuídos ou se você estiver usando DS460C compartimentos de disco na sua configuração, será necessário atribuir discos a cada um dos nós na configuração do MetroCluster de acordo com compartimento a compartimento. Você criará uma configuração na qual cada nó tem o mesmo número de discos em seus pools de discos locais e remotos.

Antes de começar

Os controladores de armazenamento têm de estar no modo de manutenção.

Sobre esta tarefa

Se a configuração não incluir DS460C compartimentos de disco, essa tarefa não será necessária se os discos tiverem sido atribuídos corretamente quando recebidos de fábrica.

O pool 0 sempre contém os discos que são encontrados no mesmo local do sistema de armazenamento que os possui.

O pool 1 sempre contém os discos que são remotos para o sistema de storage que os possui.

Se a configuração incluir DS460C compartimentos de disco, você deve atribuir manualmente os discos usando as seguintes diretrizes para cada gaveta de 12 discos:

Atribuir estes discos na gaveta…	Para este nó e pool…
0 - 2	Pool do nó local 0
3 - 5	Pool do nó de PARCEIRO HA 0
6 - 8	Parceiro de DR do pool de nós locais 1
9 - 11	Parceiro de DR do pool de parceiros de HA 1

Esse padrão de atribuição de disco garante que um agregado seja minimamente afetado caso uma gaveta fique offline.

Passos

1. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.
2. Atribua os compartimentos de disco aos nós localizados no primeiro local (local A):

   Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1.

   Você deve atribuir um número igual de prateleiras a cada pool.

   a. No primeiro nó, atribua sistematicamente as gavetas de disco locais ao pool 0 e às gavetas de disco remotas ao pool 1:

      `disk assign -shelf local-switch-name:shelf-name.port -p pool`

      Se o controlador de storage Controller_A_1 tiver quatro compartimentos, você emitirá os seguintes comandos:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
      ```

   b. Repita o processo para o segundo nó no local, atribuindo sistematicamente as gavetas de disco locais

ao pool 0 e as gavetas de disco remotas ao pool 1:

`disk assign -shelf local-switch-name:shelf-name.port -p pool`

Se o controlador de storage Controller_A_2 tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Atribua os compartimentos de disco aos nós localizados no segundo local (local B):

Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1.

Você deve atribuir um número igual de prateleiras a cada pool.

a. No primeiro nó no local remoto, atribua sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1:

`disk assign -shelf local-switch-nameshelf-name -p pool`

Se o controlador de storage Controller_B_1 tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. Repita o processo para o segundo nó no local remoto, atribuindo sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1:

`disk assign -shelf shelf-name -p pool`

Se o controlador de storage Controller_B_2 tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirme as atribuições do compartimento:

   ```
   storage show shelf
   ```

5. Sair do modo de manutenção:

   ```
   halt
   ```

6. Apresentar o menu de arranque:

   ```
   boot_ontap menu
   ```

7. Em cada nó, selecione a opção **4** para inicializar todos os discos.

Atribuição de propriedade de disco em sistemas AFF

Se você estiver usando sistemas AFF em uma configuração com agregados espelhados e os nós não tiverem os discos (SSDs) corretamente atribuídos, atribua metade dos discos em cada gaveta a um nó local e a outra metade dos discos a seu nó de parceiro de HA. Você deve criar uma configuração na qual cada nó tenha o mesmo número de discos em seus pools de discos locais e remotos.

Antes de começar

Os controladores de armazenamento têm de estar no modo de manutenção.

Sobre esta tarefa

Isso não se aplica a configurações que tenham agregados sem espelhamento, uma configuração ativo/passivo ou que tenham um número desigual de discos em pools locais e remotos.

Esta tarefa não é necessária se os discos tiverem sido corretamente atribuídos quando recebidos de fábrica.

> O pool 0 sempre contém os discos que são encontrados no mesmo local do sistema de armazenamento que os possui.
>
> O pool 1 sempre contém os discos que são remotos para o sistema de storage que os possui.

Passos

1. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.
2. Atribua os discos aos nós localizados no primeiro local (local A):

   Você deve atribuir um número igual de discos a cada pool.

   a. No primeiro nó, atribua sistematicamente metade dos discos em cada gaveta ao pool 0 e a outra metade ao pool 0 do parceiro de HA:

      ```
      disk assign -shelf <shelf-name> -p <pool> -n <number-of-disks>
      ```

      Se o controlador de storage Controller_A_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Repita o processo para o segundo nó no local, atribuindo sistematicamente metade dos discos em cada gaveta ao pool 1 e a outra metade ao pool 1 do parceiro de HA:

`disk assign -disk disk-name -p pool`

Se o controlador de storage Controller_A_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Atribua os discos aos nós localizados no segundo local (local B):

Você deve atribuir um número igual de discos a cada pool.

a. No primeiro nó no local remoto, atribua sistematicamente metade dos discos em cada gaveta ao pool 0 e a outra metade ao pool 0 do parceiro de HA:

`disk assign -disk *disk-name* -p *pool*`

Se o controlador de storage Controller_B_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. Repita o processo para o segundo nó no local remoto, atribuindo sistematicamente metade dos discos em cada gaveta ao pool 1 e a outra metade ao pool 1 do parceiro de HA:

`disk assign -disk *disk-name* -p *pool*`

Se o controlador de storage Controller_B_2 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirme as atribuições de disco:

   ```
   storage show disk
   ```

5. Sair do modo de manutenção:

   ```
   halt
   ```

6. Apresentar o menu de arranque:

   ```
   boot_ontap menu
   ```

7. Em cada nó, selecione a opção **4** para inicializar todos os discos.

Verificando a atribuição de discos no modo Manutenção em uma configuração de dois nós

Antes de iniciar totalmente o sistema no ONTAP, você pode opcionalmente inicializar o sistema no modo Manutenção e verificar a atribuição de disco nos nós. Os discos devem ser atribuídos para criar uma configuração totalmente simétrica, com os dois locais que possuem suas próprias gavetas de disco e fornecimento de dados, em que cada nó e cada pool têm um número igual de discos espelhados atribuídos a eles.

Antes de começar

O sistema tem de estar no modo de manutenção.

Sobre esta tarefa

Os novos sistemas MetroCluster têm atribuição de disco concluída antes do envio.

A tabela a seguir mostra exemplos de atribuições de pool para uma configuração do MetroCluster. Os discos são atribuídos a pools por compartimento.

Compartimento de disco (nome do exemplo)…	No local…	Pertence a…	E é atribuído a esse nó…
Compartimento de disco 1 (shelf_A_1_1)	Local A	Nó A 1	Piscina 0
Compartimento de disco 2 (shelf_A_1_3)			
Compartimento de disco 3 (gaveta_B_1_1)		Nó B 1	Piscina 1
Compartimento de disco 4 (gaveta_B_1_3)			

Compartimento de disco 9 (gaveta_B_1_2)	Local B	Nó B 1	Piscina 0
Compartimento de disco 10 (gaveta_B_1_4)			
Compartimento de disco 11 (shelf_A_1_2)		Nó A 1	Piscina 1
Compartimento de disco 12 (shelf_A_1_4)			

Se a configuração incluir DS460C compartimentos de disco, você deve atribuir manualmente os discos usando as seguintes diretrizes para cada gaveta de 12 discos:

Atribuir estes discos na gaveta…	Para este nó e pool…
1 - 6	Pool do nó local 0
7 - 12	Pool do parceiro DR 1

Esse padrão de atribuição de disco minimiza o efeito em um agregado se uma gaveta ficar offline.

Passos

1. Se o seu sistema foi recebido de fábrica, confirme as atribuições de prateleira:

   ```
   disk show –v
   ```

2. Se necessário, você pode atribuir explicitamente discos nas gavetas de disco conetadas ao pool apropriado usando o comando Disk Assign.

   Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1. Você deve atribuir um número igual de prateleiras a cada pool.

   a. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.

   b. No nó no Local A, atribua sistematicamente as gavetas de disco locais ao pool 0 e às gavetas de disco remotas ao pool 1:

      ```
      disk assign -shelf disk_shelf_name -p pool
      ```

      Se o nó_A_1 do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

      ```
      *> disk assign -shelf shelf_A_1_1 -p 0
      *> disk assign -shelf shelf_A_1_3 -p 0

      *> disk assign -shelf shelf_A_1_2 -p 1
      *> disk assign -shelf shelf_A_1_4 -p 1
      ```

   c. No nó do local remoto (local B), atribua sistematicamente seus compartimentos de disco locais ao pool

0 e suas gavetas de disco remotas ao pool 1:

`disk assign -shelf disk_shelf_name -p pool`

Se o nó_B_1 do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf shelf_B_1_2   -p 0
*> disk assign -shelf shelf_B_1_4  -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
 *> disk assign -shelf shelf_B_1_3 -p 1
```

a. Mostrar as IDs e os compartimentos do compartimento de disco para cada disco:

`disk show -v`

Configurar o ONTAP

Tem de configurar o ONTAP em cada módulo do controlador.

Se você precisar netboot dos novos controladores, consulte "Netbooting os novos módulos do controlador" no *MetroCluster Upgrade, Transition e Expansion Guide*.

Opções

- Configurando o ONTAP em uma configuração de MetroCluster de dois nós
- Configurando o ONTAP em uma configuração MetroCluster de oito ou quatro nós

Configurando o ONTAP em uma configuração de MetroCluster de dois nós

Em uma configuração de MetroCluster de dois nós, em cada cluster, você deve inicializar o nó, sair do assistente de configuração de cluster e usar o comando de configuração de cluster para configurar o nó em um cluster de nó único.

Antes de começar

Você não deve ter configurado o processador de serviço.

Sobre esta tarefa

Essa tarefa é para configurações de MetroCluster de dois nós que usam storage nativo do NetApp.

Essa tarefa deve ser executada em ambos os clusters na configuração do MetroCluster.

Para obter mais informações gerais sobre a configuração do ONTAP, "Configure o ONTAP"consulte .

Passos

1. Ligue o primeiro nó.

   Repita esta etapa no nó no local de recuperação de desastres (DR).

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

que o AutoSupport será ativado automaticamente.

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

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



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

2. Criar um novo cluster:

```
create
```

3. Escolha se o nó deve ser usado como um cluster de nó único.

```
Do you intend for this node to be used as a single node cluster? {yes,
no} [yes]:
```

4. Aceite o padrão do sistema `yes` pressionando Enter ou insira seus próprios valores digitando `no`e pressionando Enter.
5. Siga as instruções para concluir o assistente **Configuração de cluster**, pressione Enter para aceitar os valores padrão ou digitar seus próprios valores e pressione Enter.

   Os valores padrão são determinados automaticamente com base na sua plataforma e configuração de rede.

6. Depois de concluir o assistente **Cluster Setup** e ele sair, verifique se o cluster está ativo e se o primeiro nó está saudável: "

   `cluster show`

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

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

   Se for necessário alterar qualquer uma das configurações inseridas para o SVM admin ou nó SVM, você poderá acessar o assistente Configuração de cluster usando o comando de configuração de cluster.

Configuração do ONTAP em uma configuração de MetroCluster de oito ou quatro nós

Depois de inicializar cada nó, você será solicitado a executar a ferramenta Configuração do sistema para executar a configuração básica do nó e do cluster. Depois de configurar o cluster, você retorna à CLI do ONTAP para criar agregados e criar a configuração do MetroCluster.

Antes de começar

Você deve ter cabeado a configuração do MetroCluster.

Sobre esta tarefa

Essa tarefa é para configurações de MetroCluster de oito ou quatro nós que usam storage NetApp nativo.

Os novos sistemas MetroCluster estão pré-configurados; não é necessário executar estas etapas. No entanto, você deve configurar a ferramenta AutoSupport.

Essa tarefa deve ser executada em ambos os clusters na configuração do MetroCluster.

Este procedimento utiliza a ferramenta System Setup (Configuração do sistema). Se desejar, você pode usar o assistente de configuração do cluster da CLI.

Passos

1. Se você ainda não fez isso, ligue cada nó e deixe-os inicializar completamente.

   Se o sistema estiver no modo Manutenção, emita o comando halt para sair do modo Manutenção e, em seguida, emita o seguinte comando a partir do prompt Loader:

   `boot_ontap`

A saída deve ser semelhante ao seguinte:

```
Welcome to node setup

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
                Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. Ative a ferramenta AutoSupport seguindo as instruções fornecidas pelo sistema.
3. Responda aos prompts para configurar a interface de gerenciamento de nós.

   Os prompts são semelhantes aos seguintes:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Confirme se os nós estão configurados no modo de alta disponibilidade:

   `storage failover show -fields mode`

   Caso contrário, você deve emitir o seguinte comando em cada nó e reinicializar o nó:

   `storage failover modify -mode ha -node localhost`

   Este comando configura o modo de alta disponibilidade, mas não ativa o failover de armazenamento. O failover de storage é ativado automaticamente quando a configuração do MetroCluster é executada posteriormente no processo de configuração.

5. Confirme se você tem quatro portas configuradas como interconexões de cluster:

   `network port show`

   O exemplo a seguir mostra a saída para cluster_A:

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Se você estiver criando um cluster de dois nós (um cluster sem switches de interconexão de cluster), ative o modo de rede sem switch-cluster:

   a. Mude para o nível de privilégio avançado:

      ```
      set -privilege advanced
      ```

   Você pode responder `y` quando solicitado a continuar no modo avançado. O prompt do modo avançado é exibido (*>).

   a. Ativar o modo sem switch-cluster:

      ```
      network options switchless-cluster modify -enabled true
      ```

   b. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

7. Inicie a ferramenta System Setup (Configuração do sistema) conforme indicado pelas informações que aparecem no console do sistema após a inicialização.

8. Use a ferramenta Configuração do sistema para configurar cada nó e criar o cluster, mas não criar agregados.

   Você cria agregados espelhados em tarefas posteriores.

Depois de terminar

Retorne à interface da linha de comando ONTAP e conclua a configuração do MetroCluster executando as tarefas a seguir.

Configuração dos clusters em uma configuração do MetroCluster

É necessário fazer peer nos clusters, espelhar os agregados raiz, criar um agregado de dados espelhados e, em seguida, emitir o comando para implementar as operações do MetroCluster.

Sobre esta tarefa

Antes de executar `metrocluster configure`o , o modo HA e o espelhamento de DR não estão ativados e você pode ver uma mensagem de erro relacionada a esse comportamento esperado. Você ativa o modo HA e o espelhamento de DR mais tarde quando executa o comando `metrocluster configure` para implementar a configuração.

Peering dos clusters

Os clusters na configuração do MetroCluster precisam estar em um relacionamento de mesmo nível para que possam se comunicar uns com os outros e executar o espelhamento de dados essencial para a recuperação de desastres do MetroCluster.

Configurando LIFs entre clusters

É necessário criar LIFs entre clusters nas portas usadas para comunicação entre os clusters de parceiros da MetroCluster. Você pode usar portas dedicadas ou portas que também têm tráfego de dados.

Opções

- Configurando LIFs entre clusters em portas dedicadas
- Configurando LIFs entre clusters em portas de dados compartilhados

Configurando LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede em "cluster01":

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que as portas "e0e" e "e0f" não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports`

O exemplo a seguir atribui as portas "e0e" e "e0f" ao grupo de failover intercluster01 no sistema "SVMcluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

`network interface failover-groups show`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

ONTAP 9 F.6 e mais tarde

```
network interface create -vserver system_SVM -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP
-netmask netmask -failover-group failover_group
```

ONTAP 9 F.5 e anteriores

```
network interface create -vserver system_SVM -lif LIF_name -role
intercluster -home-node node -home-port port -address port_IP -netmask
netmask -failover-group failover_group
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" no grupo de failover "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

ONTAP 9 F.6 e mais tarde

Execute o comando: `network interface show -service-policy default-intercluster`

ONTAP 9 F.5 e anteriores

Execute o comando: `network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verifique se as LIFs entre clusters são redundantes:

ONTAP 9 F.6 e mais tarde

Execute o comando: `network interface show -service-policy default-intercluster -failover`

ONTAP 9 F.5 e anteriores

Execute o comando: `network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta SVM "e0e" falharão para a porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Informações relacionadas

"Considerações ao usar portas dedicadas"

Ao determinar se o uso de uma porta dedicada para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, banda WAN disponível, intervalo de replicação, taxa de alteração e número de portas.

Configurando LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

   ```
   cluster01::> network port show
                                                                  Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Criar LIFs entre clusters no sistema:

ONTAP 9 F.6 e mais tarde

Execute o comando: `network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask`

ONTAP 9 F.5 e anteriores

Execute o comando:
`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask`

Para obter a sintaxe completa do comando, consulte a página man. O exemplo a seguir cria LIFs entre clusters cluster01_icl01 e cluster01_icl02:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

ONTAP 9 F.6 e mais tarde

Execute o comando: `network interface show -service-policy default-intercluster`

ONTAP 9 F.5 e anteriores

Execute o comando: `network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

ONTAP 9 F.6 e mais tarde

Execute o comando: `network interface show –service-policy default-intercluster -failover`

ONTAP 9 F.5 e anteriores

Execute o comando:
`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "e0c" falharão para a porta "e0d".

```
cluster01::> network interface show -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Informações relacionadas

"Considerações ao compartilhar portas de dados"

Criando um relacionamento de cluster peer

É necessário criar o relacionamento de peers de clusters entre os clusters do MetroCluster.

Sobre esta tarefa

Você pode usar o `cluster peer create` comando para criar uma relação entre pares entre um cluster local e remoto. Após a criação da relação de pares, você pode executar `cluster peer create` no cluster remoto para autenticá-la no cluster local.

Antes de começar

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior.

Passos

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

   `cluster peer create -generate-passphrase -offer-expiration` *`MM/DD/YYYY HH:MM:SS|1…7days|1…168hours`* `-peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Se você especificar ambos `-generate-passphrase` e `-peer-addrs`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addrs` poderá usar a senha gerada.

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um relacionamento de peer de cluster em um cluster remoto não especificado:

   ```
   cluster02::> cluster peer create -generate-passphrase -offer-expiration
   2days

                       Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                 Expiration Time: 6/7/2017 08:16:10 EST
     Initial Allowed Vserver Peers: -
               Intercluster LIF IP: 192.140.112.101
                 Peer Cluster Name: Clus_7ShR (temporary generated)

   Warning: make a note of the passphrase - it cannot be displayed again.
   ```

2. No cluster de origem, autentique o cluster de origem no cluster de destino:

   `cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autentica o cluster local para o cluster remoto em endereços IP de LIF "192.140.112.101" e "192.140.112.102":

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                               Last Update Time: 02/05 21:05:41
                   IPspace for the Relationship: Default
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Criando um relacionamento de cluster peer (ONTAP 9.2 e anterior)

Você pode usar o `cluster peer create` comando para iniciar uma solicitação de um relacionamento de peering entre um cluster local e remoto. Depois que o relacionamento de pares tiver sido solicitado pelo cluster local, você pode executar `cluster peer create` no cluster remoto para aceitar o relacionamento.

Antes de começar

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os administradores de cluster devem ter concordado com a frase-passe que cada cluster usará para se autenticar com o outro.

Passos

1. No cluster de destino de proteção de dados, crie uma relação de mesmo nível com o cluster de origem de proteção de dados:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Você pode ignorar a opção *-ipspace* se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria uma relação de peer de cluster com o cluster remoto em endereços IP de LIF "192.168.2.201" e "192.168.2.202":

```
cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
Enter the passphrase:
Please enter the passphrase again:
```

Digite a senha para o relacionamento de pares quando solicitado.

2. No cluster de origem de proteção de dados, autentique o cluster de origem no cluster de destino:

   `cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autentica o cluster local para o cluster remoto em endereços IP de LIF "192.140.112.203" e "192.140.112.204":

   ```
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

   `cluster peer show –instance`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster01::> cluster peer show –instance
   Peer Cluster Name: cluster01
   Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
   Availability: Available
   Remote Cluster Name: cluster02
   Active IP Addresses: 192.168.2.201,192.168.2.202
   Cluster Serial Number: 1-80-000013
   ```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

   `cluster peer health show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Espelhamento dos agregados de raiz

É necessário espelhar os agregados raiz para fornecer proteção de dados.

Sobre esta tarefa

Por padrão, o agregado raiz é criado como agregado do tipo RAID-DP. Você pode alterar o agregado raiz de RAID-DP para o agregado do tipo RAID4. O comando a seguir modifica o agregado raiz para o agregado do tipo RAID4:

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```

Em sistemas que não sejam ADP, o tipo RAID do agregado pode ser modificado do RAID-DP padrão para RAID4 antes ou depois que o agregado é espelhado.

Passos

1. Espelhar o agregado raiz:

   ```
   storage aggregate mirror aggr_name
   ```

   O comando a seguir espelha o agregado raiz para controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Isso reflete o agregado, por isso consiste em um Plex local e um Plex remoto localizado no local remoto

de MetroCluster.

2. Repita a etapa anterior para cada nó na configuração do MetroCluster.

Informações relacionadas

"Gerenciamento de storage lógico com a CLI"

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.
- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster. "Gerenciamento de disco e agregado"Consulte .

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   ```
   storage disk show -spare -owner node_name
   ```

2. Crie o agregado usando o comando storage Aggregate create -mirror true.

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para garantir que o agregado seja criado em um nó específico, use o `-node` parâmetro ou especifique as unidades que são de propriedade desse nó.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
   - Número de unidades a incluir

   > Na configuração com suporte mínimo, na qual um número limitado de unidades está disponível, você deve usar a `force-small-aggregate` opção para permitir a criação de um agregado RAID-DP de três discos.

   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
   - Se unidades com RPM diferentes são permitidas

Para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Criação de agregados de dados sem espelhamento

Você pode, opcionalmente, criar agregados de dados sem espelhamento para dados que não exigem o espelhamento redundante fornecido pelas configurações do MetroCluster.

Antes de começar

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode verificar se o tipo de unidade correto está selecionado.

> Nas configurações de FC MetroCluster, os agregados sem espelhamento só estarão online após um switchover se os discos remotos no agregado estiverem acessíveis. Se os ISLs falharem, o nó local poderá não conseguir aceder aos dados nos discos remotos sem espelhamento. A falha de um agregado pode levar a uma reinicialização do nó local.

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.

> Os agregados sem espelhamento devem ser locais para o nó que os possui.

- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.
- *Gerenciamento de discos e agregados* contém mais informações sobre o espelhamento de agregados.

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   `storage disk show -spare -owner` *`node_name`*

2. Criar o agregado:

   `storage aggregate create`

Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para verificar se o agregado é criado em um nó específico, você deve usar o `-node` parâmetro ou especificar unidades que são de propriedade desse nó.

Você pode especificar as seguintes opções:

- Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
- Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
- Número de unidades a incluir
- Estilo de checksum para usar para o agregado
- Tipo de unidades a utilizar
- Tamanho das unidades a utilizar
- Velocidade de condução a utilizar
- Tipo RAID para grupos RAID no agregado
- Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
- Se unidades com RPM diferentes são permitidas

Para obter mais informações sobre essas opções, consulte a página de manual criar agregado de armazenamento.

O comando a seguir cria um agregado sem espelhamento com 10 discos:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Informações relacionadas

"Gerenciamento de disco e camada (agregado)"

Implementando a configuração do MetroCluster

Você deve executar o `metrocluster configure` comando para iniciar a proteção de dados em uma configuração do MetroCluster.

Antes de começar

- Deve haver pelo menos dois agregados de dados espelhados não-raiz em cada cluster.

  Agregados de dados adicionais podem ser espelhados ou sem espelhamento.

  Você pode verificar isso com o `storage aggregate show` comando.

Se você quiser usar um único agregado de dados espelhados, consulte Passo 1 para obter instruções.

- O estado ha-config dos controladores e chassis deve ser "mcc".

Sobre esta tarefa

Você emite o `metrocluster configure` comando uma vez, em qualquer um dos nós, para ativar a configuração do MetroCluster. Você não precisa emitir o comando em cada um dos sites ou nós, e não importa em qual nó ou site você escolher emitir o comando.

`metrocluster configure`O comando emparelhará automaticamente os dois nós com as IDs de sistema mais baixas em cada um dos dois clusters como parceiros de recuperação de desastres (DR). Em uma configuração de MetroCluster de quatro nós, há dois pares de parceiros de DR. O segundo par de DR é criado a partir dos dois nós com IDs de sistema mais altas.

Você deve configurar o OKM (Onboard Key Manager) ou o gerenciamento de chaves externas antes de executar o comando `metrocluster configure`.

Passos

1. Configure o MetroCluster no seguinte formato:

Se a sua configuração do MetroCluster tiver…	Então faça isso…
Vários agregados de dados	A partir do prompt de qualquer nó, configure o MetroCluster: `metrocluster configure node-name`
Um único agregado de dados espelhados	a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado: `set -privilege advanced` Você precisa responder `y` quando for solicitado a continuar no modo avançado e você vir o prompt do modo avançado (*>). b. Configure o MetroCluster com o `-allow-with -one-aggregate true` parâmetro: `metrocluster configure -allow-with -one-aggregate true` *`node-name`* c. Voltar ao nível de privilégio de administrador: `set -privilege admin`

A prática recomendada é ter vários agregados de dados. Se o primeiro grupo de DR tiver apenas um agregado e quiser adicionar um grupo de DR com um agregado, mova o volume de metadados do agregado de dados único. Para obter mais informações sobre este procedimento, "Movimentação de um volume de metadados nas configurações do MetroCluster"consulte .

O comando a seguir habilita a configuração do MetroCluster em todos os nós do grupo DR que contém controller_A_1:

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verifique o status da rede no local A:

```
network port show
```

O exemplo a seguir mostra o uso da porta de rede em uma configuração MetroCluster de quatro nós:

```
cluster_A::> network port show
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.

   a. Verifique a configuração do local A:

```
metrocluster show
```

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Verifique a configuração a partir do local B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-disaster
```

Configuração da entrega em ordem ou entrega fora de ordem de quadros no software ONTAP

Você deve configurar a entrega em ordem (IOD) ou entrega fora de ordem (OOD) de quadros de acordo com a configuração do switch Fibre Channel (FC).

Sobre esta tarefa

Se o switch FC estiver configurado para IOD, o software ONTAP deverá ser configurado para IOD. Da mesma forma, se o switch FC estiver configurado para ODE, o ONTAP deverá ser configurado para ODE.

É necessário reiniciar o controlador para alterar a configuração.

Passo

1. Configure o ONTAP para operar IOD ou OID de quadros.
   - Por padrão, o IOD de quadros é ativado no ONTAP. Para verificar os detalhes de configuração:
     i. Entrar no modo avançado:

```
set advanced
```

ii. Verifique as configurações:

```
metrocluster interconnect adapter show
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

◦ As etapas a seguir devem ser executadas em cada nó para configurar OID de quadros:

i. Entrar no modo avançado:

```
set advanced
```

ii. Verifique as configurações do MetroCluster:

```
metrocluster interconnect adapter show
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

iii. Ative O OOD no nó "CC4-B1" e no nó "CC4-B2":

```
metrocluster interconnect adapter modify -node node_name -is-ood-enabled
true
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true
```

i. Reinicie o controlador executando um takeover de alta disponibilidade (HA) em ambas as direções.

ii. Verifique as configurações:

```
metrocluster interconnect adapter show
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                            Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI   Up     true      17.0.1.2       6a
mcc4-b1      fcvi_device_1   FC-VI   Up     true      18.0.0.2      6b
mcc4-b1      mlx4_0          IB      Down   false     192.0.5.193   ib2a
mcc4-b1      mlx4_0          IB      Up     false     192.0.5.194   ib2b
mcc4-b2      fcvi_device_0   FC-VI   Up     true      17.0.2.2      6a
mcc4-b2      fcvi_device_1   FC-VI   Up     true      18.0.1.2      6b
mcc4-b2      mlx4_0          IB      Down   false     192.0.2.9     ib2a
mcc4-b2      mlx4_0          IB      Up     false     192.0.2.10    ib2b
8 entries were displayed.
```

Configurando o SNMPv3 em uma configuração MetroCluster

Antes de começar

Os protocolos de autenticação e privacidade nos switches e no sistema ONTAP devem ser os mesmos.

Sobre esta tarefa

O ONTAP atualmente suporta criptografia AES-128.

Passos

1. Crie um usuário SNMP para cada switch a partir do prompt do controlador:

   `security login create`

   ```
   Controller_A_1::> security login create -user-or-group-name snmpv3user
   -application snmp -authentication-method usm -role none -remote-switch
   -ipaddress 10.10.10.10
   ```

2. Responda às seguintes instruções, conforme necessário, no seu site:

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

O mesmo nome de usuário pode ser adicionado a diferentes switches com endereços IP diferentes.

3. Crie um usuário SNMP para o resto dos switches.

   O exemplo a seguir mostra como criar um nome de usuário para um switch com o endereço IP 10.10.10.11.

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.
10.10.11
```

4. Verifique se há uma entrada de login para cada switch:

```
security login show
```

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

------------ ------------------ ----------- --------------------
----------------------

node_A_1 SVM 1 snmpv3user     snmp        usm
10.10.10.10

node_A_1 SVM 2 snmpv3user     snmp        usm
10.10.10.11

node_A_1 SVM 3 snmpv3user    snmp        usm
10.10.10.12

node_A_1 SVM 4 snmpv3user     snmp        usm
10.10.10.13

4 entries were displayed.
```

5. Configure o SNMPv3 nos switches a partir do prompt do switch:

Switches Brocade

```
snmpconfig --set snmpv3
```

Switches Cisco

```
snmp-server user <user_name> auth [md5/sha/sha-256] <auth_password> priv
(aes-128) <priv_password>
```

Se você precisar de acesso RO, depois de "Usuário (ro):" especifique "snmpv3user". O exemplo a seguir usa switches Brocade:

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user database
will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [3]
```

O exemplo mostra como configurar um usuário somente leitura. Você pode ajustar os usuários RW, se necessário.

Você também deve definir senhas em contas não utilizadas para protegê-las e usar a melhor criptografia disponível em sua versão do ONTAP.

6. Configure criptografia e senhas nos demais usuários do switch, conforme necessário em seu site.

Configuração de componentes do MetroCluster para monitoramento de integridade

Você deve executar algumas etapas especiais de configuração antes de monitorar os componentes em uma configuração do MetroCluster.

Sobre esta tarefa

Essas tarefas se aplicam somente a sistemas com pontes FC para SAS.

A partir do Fabric os 9,0.1, o SNMPv2 não é suportado para monitoramento de integridade em switches Brocade, você deve usar o SNMPv3 em vez disso. Se você estiver usando SNMPv3, você deve configurar o SNMPv3 no ONTAP antes de prosseguir para a seção a seguir. Para obter mais detalhes, Configurando o SNMPv3 em uma configuração MetroClusterconsulte .

- Você deve colocar bridges e um LIF de gerenciamento de nós em uma rede dedicada para evitar interferência de outras fontes.
- Se você usar uma rede dedicada para monitoramento de integridade, cada nó deve ter um LIF de gerenciamento de nós nessa rede dedicada.

O NetApp oferece suporte apenas às seguintes ferramentas para monitorar os componentes em uma configuração do MetroCluster FC:

- Consultor de rede Brocade (BNA)
- Brocade SANnav
- Active IQ Config Advisor
- Monitoramento NetApp de Saúde (ONTAP)
- Coletor de dados MetroCluster (MC_DC)

Configuração dos switches MetroCluster FC para monitoramento de integridade

Em uma configuração do MetroCluster conectado à malha, você precisa executar algumas etapas adicionais de configuração para monitorar os switches FC.

> A partir de ONTAP 9.8, o `storage switch` comando é substituído por `system switch`. As etapas a seguir mostram o `storage switch` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system switch` comando é preferido.

Passos

1. Adicione um switch com um endereço IP a cada nó do MetroCluster:

   O comando executado depende se você está usando SNMPv2 ou SNMPv3.

   Adicione um switch usando SNMPv3:

   ```
   storage switch add -address <ip_adddress> -snmp-version SNMPv3 -snmp
   -community-or-username <SNMP_user_configured_on_the_switch>
   ```

   Adicione um switch usando SNMPv2:

   ```
   storage switch add -address ipaddress
   ```

   Este comando deve ser repetido em todos os quatro switches na configuração MetroCluster.

   > Os switches Brocade 7840 FC e todos os alertas são compatíveis com monitoramento de integridade, exceto NoISLPresent_Alert.

   O exemplo a seguir mostra o comando para adicionar um switch com endereço IP 10.10.10.10:

   ```
   controller_A_1::> storage switch add -address 10.10.10.10
   ```

2. Verifique se todos os switches estão configurados corretamente:

   ```
   storage switch show
   ```

   Pode levar até 15 minutos para refletir todos os dados devido ao intervalo de votação de 15 minutos.

   O exemplo a seguir mostra o comando dado para verificar se os switches MetroCluster FC estão configurados:

```
controller_A_1::> storage switch show
Fabric           Switch Name     Vendor  Model        Switch WWN
Status
---------------- --------------- ------- ------------ ----------------
------
1000000533a9e7a6 brcd6505-fcs40  Brocade Brocade6505  1000000533a9e7a6
OK
1000000533a9e7a6 brcd6505-fcs42  Brocade Brocade6505  1000000533d3660a
OK
1000000533ed94d1 brcd6510-fcs44  Brocade Brocade6510  1000000533eda031
OK
1000000533ed94d1 brcd6510-fcs45  Brocade Brocade6510  1000000533ed94d1
OK
4 entries were displayed.

controller_A_1::>
```

Se o nome mundial (WWN) do switch for exibido, o monitor de integridade do ONTAP pode entrar em Contato e monitorar o switch FC.

Informações relacionadas

"Administração do sistema"

Configuração de pontes FC para SAS para monitoramento de integridade

Em sistemas que executam versões do ONTAP anteriores a 9,8, você deve executar algumas etapas especiais de configuração para monitorar as pontes FC para SAS na configuração do MetroCluster.

Sobre esta tarefa

- Ferramentas de monitoramento SNMP de terceiros não são suportadas para bridges FibreBridge.
- A partir do ONTAP 9.8, as bridges FC para SAS são monitoradas por meio de conexões na banda por padrão, e não é necessária configuração adicional.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

   a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
9,5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*

9,4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

b. Verifique se a ponte foi adicionada e está configurada corretamente:

`storage bridge show`

Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de integridade do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente.

Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster. Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Sobre esta tarefa

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Comandos subsequentes `metrocluster check show`, então não mostrará a saída esperada.

Passos

1. Verificar a configuração:

   `metrocluster check run`

   O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Exibir resultados mais detalhados do comando mais recente `metrocluster check run`:

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`

   `metrocluster check node show`

   > Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

   O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr2
```

```
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

O exemplo a seguir mostra a `metrocluster check cluster show` saída do comando para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

Informações relacionadas

"Gerenciamento de disco e agregado"

"Gerenciamento de rede e LIF"

Verificando erros de configuração do MetroCluster com o Config Advisor

Você pode acessar o site de suporte da NetApp e baixar a ferramenta Config Advisor para verificar se há erros de configuração comuns.

Sobre esta tarefa

O Config Advisor é uma ferramenta de validação de configuração e verificação de integridade. Você pode implantá-lo em sites seguros e sites não seguros para coleta de dados e análise do sistema.

O suporte para Config Advisor é limitado e está disponível apenas online.

Passos

1. Vá para a página de download do Config Advisor e baixe a ferramenta.

   "NetApp Downloads: Config Advisor"

2. Execute o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Verificação da operação local de HA

Se você tiver uma configuração de MetroCluster de quatro nós, verifique a operação dos pares de HA locais na configuração do MetroCluster. Isso não é necessário para configurações de dois nós.

Sobre esta tarefa

As configurações de MetroCluster de dois nós não consistem em pares de HA locais, e essa tarefa não se aplica.

Os exemplos nesta tarefa usam convenções de nomenclatura padrão:

- Cluster_A
  - controller_A_1
  - controller_A_2
- Cluster_B
  - controller_B_1
  - controller_B_2

Passos

1. Em cluster_A, execute um failover e giveback em ambas as direções.

   a. Confirme se o failover de armazenamento está ativado:

      ```
      storage failover show
      ```

      A saída deve indicar que a aquisição é possível para ambos os nós:

      ```
      cluster_A::> storage failover show
                                    Takeover
      Node           Partner        Possible State Description
      -------------- -------------- -------- -------------------------
      controller_A_1 controller_A_2 true     Connected to controller_A_2

      controller_A_2 controller_A_1 true     Connected to controller_A_1
      2 entries were displayed.
      ```

   b. Assuma o comando controller_A_2 do controller_A_1:

      ```
      storage failover takeover controller_A_2
      ```

Você pode usar o `storage failover show-takeover` comando para monitorar o andamento da operação de aquisição.

c. Confirme se a aquisição está concluída:

```
storage failover show
```

A saída deve indicar que controller_A_1 está no estado de aquisição, o que significa que assumiu o seu parceiro HA:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -----------------
controller_A_1 controller_A_2 false    In takeover

controller_A_2 controller_A_1 -        Unknown
2 entries were displayed.
```

d. Devolver o controlador_A_2:

```
storage failover giveback controller_A_2
```

Você pode usar o `storage failover show-giveback` comando para monitorar o progresso da operação de giveback.

e. Confirme se o failover de armazenamento retornou ao estado normal:

```
storage failover show
```

A saída deve indicar que a aquisição é possível para ambos os nós:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ---------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

a. Repita as subetapas anteriores, desta vez assumindo controller_A_1 do controller_A_2.

2. Repita os passos anteriores no cluster_B.

Informações relacionadas

"Configuração de alta disponibilidade"

Verificando switchover, cura e switchback

Você deve verificar as operações de switchover, recuperação e switchback da configuração do MetroCluster.

Passo

1. Use os procedimentos para comutação negociada, cura e switchback que são mencionados no "Recuperar de um desastre" .

Protegendo arquivos de backup de configuração

Você pode fornecer proteção adicional para os arquivos de backup de configuração de cluster especificando um URL remoto (HTTP ou FTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster local.

Passo

1. Defina o URL do destino remoto para os arquivos de backup de configuração:

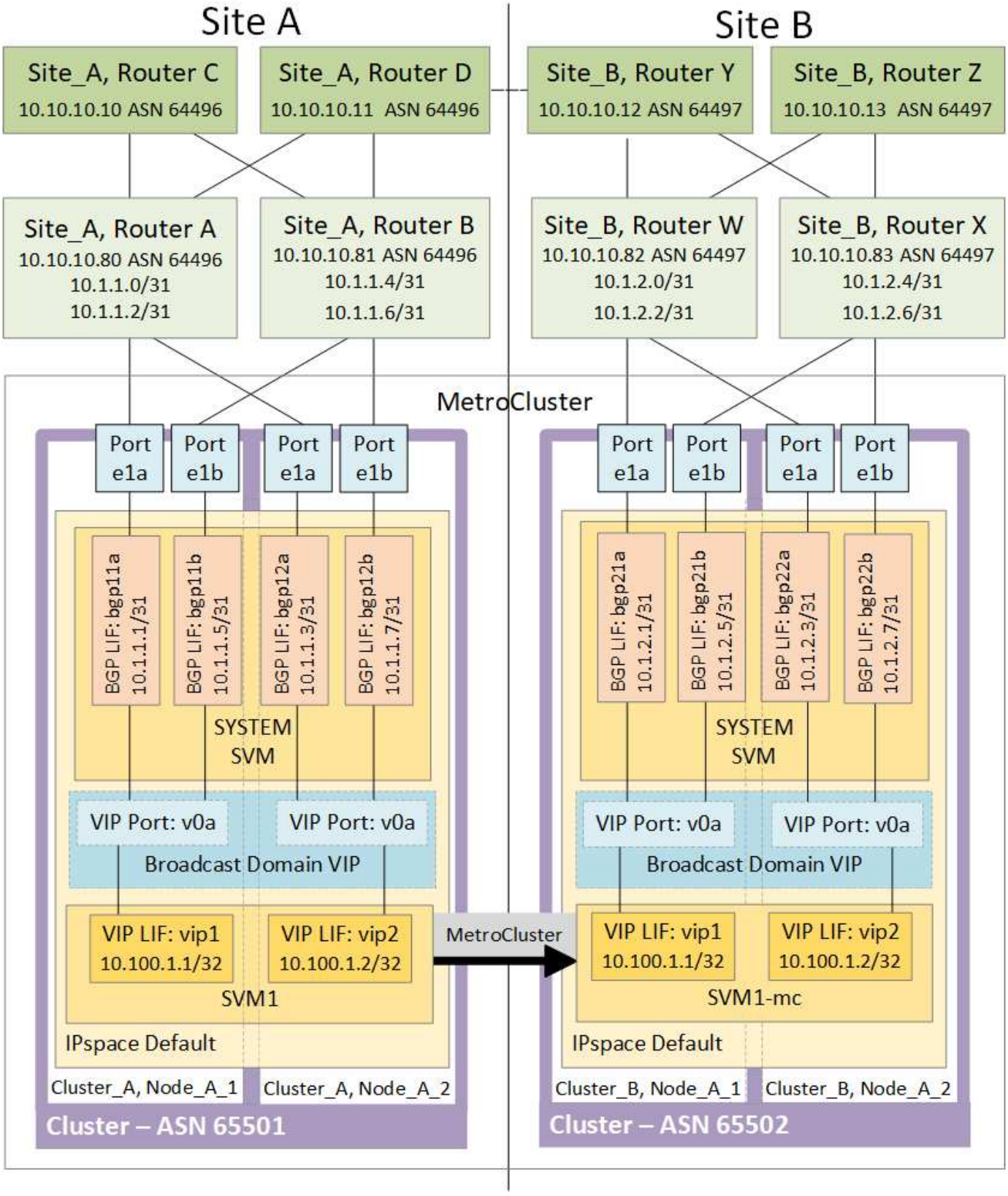
   `system configuration backup settings modify` *`URL-of-destination`*

   O "Gerenciamento de clusters com a CLI" contém informações adicionais na seção *Gerenciando backups de configuração*.

Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster

A partir do ONTAP 9.5, o ONTAP oferece suporte à conetividade da camada 3 usando IP virtual (VIP) e protocolo de gateway de borda (BGP). A combinação VIP e BGP para redundância na rede front-end com a redundância MetroCluster back-end fornece uma solução de recuperação de desastres de camada 3.

Revise as diretrizes e a ilustração a seguir ao Planejar sua solução de camada 3. Para obter detalhes sobre como implementar o VIP e o BGP no ONTAP, "Configurar IP LIFs virtuais"consulte .



Limitações DE ONTAP

O ONTAP não verifica automaticamente se todos os nós em ambos os sites da configuração do MetroCluster estão configurados com peering BGP.

O ONTAP não executa agregação de rotas, mas anuncia todos os IPs de LIF virtuais individuais como rotas de host exclusivas em todos os momentos.

O ONTAP não suporta True anycast — apenas um único nó no cluster apresenta um IP de LIF virtual específico (mas é aceito por todas as interfaces físicas, independentemente de serem LIFs BGP, desde que a porta física faça parte do espaço IPspace correto). Diferentes LIFs podem migrar independentemente um do outro para diferentes nós de hospedagem.

Diretrizes para o uso desta solução de camada 3 com uma configuração MetroCluster

Você deve configurar seu BGP e VIP corretamente para fornecer a redundância necessária.

Cenários de implantação mais simples são preferidos em relação a arquiteturas mais complexas (por exemplo, um roteador de peering BGP é acessível em um roteador intermediário não BGP). No entanto, o ONTAP não aplica restrições de design ou topologia de rede.

Os LIFs VIP cobrem apenas a rede frontend/data.

Dependendo da sua versão do ONTAP, você deve configurar LIFs de peering BGP no nó SVM, não no sistema ou na SVM de dados. No ONTAP 9.8, as LIFs de BGP são visíveis no SVM do cluster (sistema) e as SVMs de nó não estão mais presentes.

Cada SVM de dados requer a configuração de todos os endereços potenciais de gateway de primeiro salto (normalmente, o endereço IP de peering do roteador BGP), de modo que o caminho de dados de retorno esteja disponível se ocorrer uma migração de LIF ou failover de MetroCluster.

As LIFs BGP são específicas de nós, semelhantes às LIFs entre clusters - cada nó tem uma configuração exclusiva, que não precisa ser replicado para os nós do local de DR.

Uma vez configurado, a existência do v0a (v0b e assim por diante) valida continuamente a conetividade, garantindo que uma migração de LIF ou failover seja bem-sucedida (ao contrário do L2, onde uma configuração quebrada só é visível após a interrupção).

Uma grande diferença de arquitetura é que os clientes não devem mais compartilhar a mesma sub-rede IP que o VIP de SVMs de dados. Um roteador L3 com recursos apropriados de resiliência e redundância de nível empresarial habilitados (por exemplo, VRRP/HSRP) deve estar no caminho entre o armazenamento e os clientes para que o VIP funcione corretamente.

O processo de atualização confiável do BGP permite migrações de LIF mais suaves, pois elas são marginalmente mais rápidas e têm menor chance de interrupção para alguns clientes

Você pode configurar o BGP para detetar algumas classes de comportamentos incorretos de rede ou switch mais rápido do que o LACP, se configurado de acordo.

O BGP externo (EBGP) usa números diferentes entre nós ONTAP e roteadores de peering e é a implantação preferida para facilitar a agregação e redistribuição de rotas nos roteadores. O BGP interno (IBGP) e o uso de refletores de rota não são impossíveis, mas fora do escopo de uma configuração VIP direta.

Após a implantação, você deve verificar se o SVM de dados está acessível quando o LIF virtual associado é migrado entre todos os nós em cada local (incluindo switchover de MetroCluster) para verificar a configuração correta das rotas estáticas para o mesmo SVM de dados.

O VIP funciona para a maioria dos protocolos baseados em IP (NFS, SMB, iSCSI).

Testando a configuração do MetroCluster

Você pode testar cenários de falha para confirmar o funcionamento correto da configuração do MetroCluster.

Verificando o switchover negociado

Você pode testar a operação switchover negociado (planejada) para confirmar a disponibilidade de dados ininterrupta.

Sobre esta tarefa

Este teste valida que a disponibilidade de dados não é afetada (exceto para os protocolos SMB (Server Message Block) da Microsoft e Fibre Channel do Solaris), alternando o cluster para o segundo data center.

Este teste deve levar cerca de 30 minutos.

Este procedimento tem os seguintes resultados esperados:

- O `metrocluster switchover` comando apresentará um prompt de aviso.

  Se você responder `yes` ao prompt, o site do qual o comando é emitido mudará para o site do parceiro.

Para configurações IP do MetroCluster:

- Para o ONTAP 9.4 e versões anteriores:
  - Os agregados espelhados ficarão degradados após o switchover negociado.
- Para o ONTAP 9.5 e posterior:
  - Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
  - Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Para o ONTAP 9.8 e posterior:
  - Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

Passos

1. Confirme se todos os nós estão no estado configurado e no modo normal:

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                     Configuration State    Mode
--------------------------- ---------------------
-----------------------
 Local: cluster_A              configured             normal
Remote: cluster_B              configured             normal
```

2. Inicie a operação de comutação:

   `metrocluster switchover`

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "`cluster_A`". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Confirme se o cluster local está no estado configurado e no modo de comutação:

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                         Configuration State    Mode
------------------------------ ----------------------
------------------------
Local: cluster_A                configured             switchover
Remote: cluster_B               not-reachable          -
             configured             normal
```

4. Confirme se a operação de comutação foi bem-sucedida:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Use os `vserver show` comandos e `network interface show` para verificar se as SVMs e LIFs de DR estão online.

Verificando a cura e a troca manual

Você pode testar as operações de reparo e switchback manual para verificar se a disponibilidade de dados não é afetada (exceto para configurações SMB e Solaris FC), alternando o cluster para o data center original após um switchover negociado.

Sobre esta tarefa

Este teste deve levar cerca de 30 minutos.

O resultado esperado deste procedimento é que os serviços devem ser reenviados para os seus nós domésticos.

Passos

1. Verifique se a cicatrização está concluída:

   ```
   metrocluster node show
   ```

   O exemplo a seguir mostra a conclusão bem-sucedida do comando:

   ```
   cluster_A::> metrocluster node show
   DR                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ----------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   heal roots
   completed
         cluster_B
                 node_B_2         unreachable    -         switched over
   42 entries were displayed.metrocluster operation show
   ```

2. Verifique se todos os agregados estão espelhados:

   ```
   storage aggregate show
   ```

   O exemplo a seguir mostra que todos os agregados têm um status RAID espelhado:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. Inicialize os nós no local do desastre.
4. Verifique o status da recuperação de switchback:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
             node_A_1           configured     enabled   heal roots
completed
      cluster_B
             node_B_2           configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

5. Execute o interrutor de retorno:

   `metrocluster switchback`

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

6. Confirme o status dos nós:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   normal
      cluster_B
              node_B_2         configured     enabled   normal

2 entries were displayed.
```

7. Confirme o estado:

   `metrocluster operation show`

   A saída deve mostrar um estado bem-sucedido.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Perda de uma única ponte FC para SAS

Você pode testar a falha de uma única ponte FC para SAS para garantir que não haja um ponto único de falha.

Sobre esta tarefa

Este teste deve levar cerca de 15 minutos.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados quando a ponte é desligada.
- Nenhum failover ou perda de serviço deve ocorrer.
- Apenas um caminho do módulo do controlador para as unidades atrás da ponte está disponível.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Desligue as fontes de alimentação da ponte.
2. Confirme se a monitorização da ponte indica um erro:

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                                    Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
   Status
   ---------- ------------- ------- --------- ---------------- ---------
   -------
   ATTO_10.65.57.145
            bridge_A_1    Atto    FibreBridge 6500N
                                              200000108662d46c true
   error
   ```

3. Confirme se as unidades atrás da ponte estão disponíveis com um único caminho:

   `storage disk error show`

```
cluster_A::> storage disk error show
Disk             Error Type        Error Text
---------------- -----------------
-----------------------------------------
1.0.0            onedomain         1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1            onedomain         1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2            onedomain         1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23           onedomain         1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

Verificação da operação após interrupção da linha elétrica

Você pode testar a resposta da configuração do MetroCluster à falha de uma PDU.

Sobre esta tarefa

A prática recomendada é que cada unidade de fonte de alimentação (PSU) de um componente seja conetada a fontes de alimentação separadas. Se ambas as PSUs estiverem conetadas à mesma unidade de distribuição de energia (PDU) e ocorrer uma interrupção elétrica, o local pode ficar inativo ou um compartimento completo pode ficar indisponível. A falha de uma linha de alimentação é testada para confirmar que não há incompatibilidade de cabeamento que possa causar uma interrupção do serviço.

Este teste deve levar cerca de 15 minutos.

Este teste requer a desativação da energia de todas as PDUs do lado esquerdo e, em seguida, de todas as PDUs do lado direito em todos os racks que contêm os componentes do MetroCluster.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados à medida que as PDUs são desconetadas.
- Nenhum failover ou perda de serviço deve ocorrer.

Passos

1. Desligue a alimentação das PDUs no lado esquerdo do rack que contém os componentes MetroCluster.
2. Monitore o resultado no console:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- -------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Ligue a alimentação novamente para as PDUs do lado esquerdo.
4. Certifique-se de que o ONTAP limpa a condição de erro.
5. Repita os passos anteriores com as PDUs do lado direito.

Verificação da operação após uma falha na malha do switch

Você pode desativar uma malha de switch para mostrar que a disponibilidade de dados não é afetada pela perda.

Sobre esta tarefa

Este teste deve levar cerca de 15 minutos.

O resultado esperado deste procedimento é que a desativação de uma malha resulta em toda a interconexão de cluster e tráfego de disco que flui para a outra malha.

Nos exemplos mostrados, a estrutura de comutação 1 está desativada. Essa malha consiste em dois switches, um em cada local da MetroCluster:

- FC_switch_A_1 no cluster_A

- FC_switch_B_1 no cluster_B

Passos

1. Desative a conetividade com uma das duas malhas de switch na configuração do MetroCluster:

   a. Desative o primeiro switch na tela:

      `switchdisable`

      ```
      FC_switch_A_1::> switchdisable
      ```

   b. Desative o segundo interrutor na tela:

      `switchdisable`

   ```
   FC_switch_B_1::> switchdisable
   ```

2. Monitore o resultado no console dos módulos do controlador.

   Você pode usar os comandos a seguir para verificar os nós do cluster para garantir que todos os dados ainda estejam sendo atendidos. O comando output mostra caminhos ausentes para discos. Isso é esperado.

   - mostra o svm
   - mostra da interface de rede
   - aggr show
   - o storage runnodename-command do nó do sistema mostra o disco -p
   - show de erro de disco de armazenamento

3. Reative a conectividade com uma das duas malhas de switch na configuração do MetroCluster:

   a. Reative o primeiro switch na malha:

      `switchenable`

      ```
      FC_switch_A_1::> switchenable
      ```

   b. Reative o segundo switch na tela:

      `switchenable`

   ```
   FC_switch_B_1::> switchenable
   ```

4. Aguarde pelo menos 10 minutos e, em seguida, repita os passos acima na outra estrutura do interrutor.

Verificação da operação após a perda de uma única prateleira de armazenamento

Você pode testar a falha de um único compartimento de storage para verificar se não há um ponto único de falha.

Sobre esta tarefa

Este procedimento tem os seguintes resultados esperados:

- Uma mensagem de erro deve ser comunicada pelo software de monitorização.
- Nenhum failover ou perda de serviço deve ocorrer.
- A ressincronização do espelho é iniciada automaticamente após a restauração da falha de hardware.

Passos

1. Verifique o status de failover de armazenamento:

   ```
   storage failover show
   ```

   ```
   cluster_A::> storage failover show

   Node           Partner        Possible State Description
   -------------- -------------- --------
   -------------------------------------
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Verifique o status agregado:

   ```
   storage aggregate show
   ```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Verifique se todas as SVMs e volumes de dados estão on-line e fornecendo dados:

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identifique um compartimento no pool 1 para o nó node_A_2 desligar para simular uma falha repentina de hardware:

   `storage aggregate show -r -node node-name !*root`

   O compartimento selecionado deve conter unidades que fazem parte de um agregado de dados espelhados.

   No exemplo a seguir, o ID do compartimento 31 é selecionado para falhar.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                      0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                      1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                      1   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     1.31.3                        1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                        1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.5                        1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                         Pool Type     RPM     Size
Size Status
     -------- ---------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                        0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                        0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Desligue fisicamente a prateleira selecionada.
6. Verifique novamente o status do agregado:

   ```
   storage aggregate show

   storage aggregate show -r -node node_A_2 !*root
   ```

   O agregado com unidades no compartimento desligado deve ter um status RAID "desclassificado" e as unidades no Plex afetado devem ter um status de "falha", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
```

```
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
```

```
     dparity  2.30.3                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                     -   -          -  827.7GB
-  (failed)
     parity   FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                    0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     parity   2.30.22                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                    0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Verifique se os dados estão sendo fornecidos e se todos os volumes ainda estão online:

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Ligue fisicamente a prateleira.

   A ressincronização é iniciada automaticamente.

9. Verifique se a ressincronização foi iniciada:

   `storage aggregate show`

   O agregado afetado deve ter um status RAID "resincronizando", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. Monitore o agregado para confirmar que a ressincronização está concluída:

    `storage aggregate show`

    O agregado afetado deve ter um status RAID "normal", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Considerações ao remover configurações do MetroCluster

Você pode remover a configuração do MetroCluster de todos os nós na configuração do MetroCluster ou todos os nós em um grupo de recuperação de desastres (DR). Depois de remover a configuração do MetroCluster, toda a conetividade de disco e interconexões devem ser ajustadas para estar em um estado suportado. Se precisar remover a configuração do MetroCluster, entre em Contato com o suporte técnico.

Não é possível reverter a desconfiguração do MetroCluster. Este processo só deve ser feito com a assistência de suporte técnico. Entre em Contato com o suporte técnico da NetApp e consulte o guia apropriado para sua configuração no "Como remover nós de uma configuração MetroCluster - Guia de resolução."

Planejar e instalar uma configuração MetroCluster com LUNs de array

Planejando uma configuração MetroCluster com LUNs de array

A criação de um plano detalhado para a configuração do MetroCluster ajuda você a entender os requisitos exclusivos de uma configuração do MetroCluster que usa LUNs em storage arrays. A instalação de uma configuração do MetroCluster envolve a conexão e configuração de vários dispositivos, o que pode ser feito por pessoas diferentes. Portanto, o plano também ajuda você a se comunicar com outras pessoas envolvidas na instalação.

Configuração de MetroCluster compatível com LUNs de array

Você pode configurar uma configuração MetroCluster com LUNs de array. Tanto as configurações elásticas quanto as de tecido são suportadas. Os sistemas AFF não são compatíveis com LUNs de array.

Os recursos suportados nas configurações do MetroCluster variam de acordo com os tipos de configuração. A tabela a seguir lista os recursos suportados nos diferentes tipos de configurações do MetroCluster com LUNs de array:

Recurso	Configurações com conexão de malha			Configurações elásticas
	Oito nós	Quatro nós	Dois nós	Dois nós
Número de controladores	Oito	Quatro	Dois	Dois
Usa uma malha de storage de switch FC	Sim	Sim	Sim	Sim
Usa pontes FC para SAS	Sim	Sim	Sim	Sim
Suporta HA local	Sim	Sim	Não	Não
Suporta switchover automático	Sim	Sim	Sim	Sim

Informações relacionadas

"Diferenças entre as configurações do ONTAP MetroCluster"

Requisitos para uma configuração MetroCluster com LUNs de array

Os sistemas ONTAP, os storage arrays e os switches FC usados nas configurações do MetroCluster precisam atender aos requisitos desses tipos de configurações. Além disso, você também deve considerar os requisitos do SyncMirror para configurações do MetroCluster com LUNs de array.

Requisitos para sistemas ONTAP

- Os sistemas ONTAP devem ser identificados como compatíveis com configurações MetroCluster.

  No "Ferramenta de Matriz de interoperabilidade NetApp (IMT)", você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

  > Você deve consultar os detalhes de alerta associados a qualquer configuração selecionada na Matriz de interoperabilidade.

- Todos os sistemas ONTAP em uma configuração MetroCluster devem ter o mesmo modelo.
- Os adaptadores FC-VI devem ser instalados nos slots apropriados para cada sistema ONTAP, dependendo do modelo.

  "NetApp Hardware Universe"

Requisitos para matrizes de armazenamento

- Os storage arrays devem ser identificados como compatíveis com as configurações do MetroCluster.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Os storage arrays na configuração do MetroCluster devem ser simétricos:
  - Os dois storage arrays devem ser da mesma família de fornecedores com suporte e ter a mesma versão de firmware instalada.

    "Implementação de virtualização FlexArray para storage NetApp e-Series"

  "Implementação de virtualização de FlexArray para storage de terceiros"

  - Os tipos de disco (por exemplo, SATA, SSD ou SAS) usados para armazenamento espelhado devem ser os mesmos em ambas as matrizes de armazenamento.
  - Os parâmetros para configurar matrizes de armazenamento, como o tipo RAID e a disposição em camadas, devem ser os mesmos em ambos os locais.

Requisitos para switches FC

- Os switches e o firmware do switch devem ser identificados como compatíveis com configurações MetroCluster.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Cada malha precisa ter dois switches FC.
- Cada sistema ONTAP deve ser conetado ao storage usando componentes redundantes para que haja redundância em caso de falhas de dispositivo e caminho.
- Os sistemas de storage AFF A700, FAS9000, AFF A900 e FAS9500 são compatíveis com até oito ISLs por malha. Outros modelos de sistemas de storage suportam até quatro ISLs por malha.
- Os switches devem usar a configuração básica do switch MetroCluster, as configurações ISL e FC-VI.

  "Configure os switches Cisco FC manualmente"

  "Configurar manualmente os switches Brocade FC"

Requisitos da SyncMirror

- O SyncMirror é necessário para uma configuração do MetroCluster.
- Dois storage arrays separados, um em cada local, são necessários para o storage espelhado.
- São necessários dois conjuntos de LUNs de array.

  Um conjunto é necessário para o agregado no storage de armazenamento local (pool0) e outro conjunto é necessário no storage de armazenamento remoto para o espelho do agregado (o outro Plex do agregado, pool1).

  Os LUNs do array devem ter o mesmo tamanho para espelhar o agregado.
- Agregados não espelhados também são suportados na configuração MetroCluster.

  Eles não são protegidos em caso de desastre no local.

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

Instale e faça o cabeamento dos componentes do MetroCluster em uma configuração com LUNs de array

Empilhando os componentes de hardware em uma configuração MetroCluster com LUNs de matriz

Você deve garantir que os componentes de hardware necessários para configurar uma configuração MetroCluster com LUNs de array sejam corretamente montados em rack.

Sobre esta tarefa

Você deve executar esta tarefa em ambos os sites do MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   O espaço em rack depende do modelo de plataforma dos controladores de storage, dos tipos de switch e

do número de stacks de compartimento de disco na configuração.

2. Aterre-se corretamente.
3. Instale os controladores de armazenamento no rack ou gabinete.

   Os sistemas AFF não são compatíveis com LUNs de array.

   "Procedimentos de instalação para o seu sistema AFF ou FAS"

4. Instale os switches FC no rack ou gabinete.

Preparação de um storage array para uso com sistemas ONTAP

Antes de começar a configurar sistemas ONTAP em uma configuração MetroCluster com LUNs de array, o administrador do storage deve preparar o armazenamento para uso com o ONTAP.

Antes de começar

As matrizes de armazenamento, firmware e comutadores que pretende utilizar na configuração têm de ser suportadas pela versão específica do ONTAP.

- "Interoperabilidade NetApp (IMT)"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- "NetApp Hardware Universe"

Sobre esta tarefa

Você deve coordenar com o administrador do storage array para executar essa tarefa no storage array.

Passos

1. Crie LUNs no storage array, dependendo do número de nós na configuração do MetroCluster.

   Cada nó na configuração do MetroCluster requer LUNs de array para agregado de raiz, agregado de dados e peças sobressalentes.

2. Configure parâmetros no storage array que são necessários para trabalhar com o ONTAP.
   - "Implementação de virtualização de FlexArray para storage de terceiros"
   - "Implementação de virtualização FlexArray para storage NetApp e-Series"

Portas de switch necessárias para uma configuração MetroCluster com LUNs de array

Quando você conecta sistemas ONTAP a switches FC para configurar uma configuração MetroCluster com LUNs de array, é necessário conectar portas FC-VI e HBA de cada controladora a portas de switch específicas.

Se você estiver usando LUNs de array e discos na configuração MetroCluster, certifique-se de que as portas do controlador estejam conetadas às portas do switch recomendadas para configuração com discos e use as

portas restantes para configuração com LUNs de array.

A tabela a seguir lista as portas de switch FC específicas às quais você deve conectar as diferentes portas de controlador em uma configuração de MetroCluster de oito nós com LUNs de array.

Diretrizes gerais de cabeamento com LUNs de array

Você deve estar ciente das seguintes diretrizes ao usar as tabelas de cabeamento:

- Os switches Brocade e Cisco usam numeração de portas diferente:
  - Nos switches Brocade, a primeira porta é numerada 0.
  - Nos switches Cisco, a primeira porta é numerada 1.
- O cabeamento é o mesmo para cada switch FC na malha do switch.
- Os sistemas de storage FAS8200 podem ser solicitados com uma das duas opções de conectividade FC-VI:
  - Portas integradas 0e e 0f configuradas no modo FC-VI.
  - Portas 1a e 1b em uma placa FC-VI no slot 1.
- Os sistemas de storage da FAS9000 exigem quatro portas FC-VI. As tabelas a seguir mostram o cabeamento dos switches FC com quatro portas FC-VI em cada controladora.

  Para outros sistemas de armazenamento, use o cabeamento mostrado nas tabelas, mas ignore o cabeamento das portas FC-VI c e d.

  Você pode deixar essas portas vazias.

Uso de porta Brocade para controladores em uma configuração MetroCluster

As tabelas a seguir mostram o uso de portas nos switches Brocade. As tabelas mostram a configuração máxima suportada, com oito módulos de controlador em dois grupos de DR. Para configurações menores, ignore as linhas dos módulos adicionais do controlador. Observe que oito ISLs são suportadas nos switches Brocade 6510 e G620.

> O uso da porta para o switch Brocade 6505 em uma configuração MetroCluster de oito nós não é mostrado. Devido ao número limitado de portas, as atribuições de portas devem ser feitas de acordo com o modelo do módulo do controlador e o número de ISLs e pares de pontes em uso.

A tabela a seguir mostra o cabeamento do primeiro grupo de DR:

		Interrutor Brocade 6520, 6510, 6505, G620, G610 ou 7840	
Componente	**Porto**	**Switch 1**	**Switch 2**

controller_x_1	Porta a FC-VI	0	
	Porta FC-VI b	-	0
	Porta FC-VI c	1	-
	Porta d. FC-VI	-	1
	HBA porta a	2	-
	Porta HBA b	-	2
	Porta HBA c	3	-
	Porta d. HBA	-	3
controller_x_2	Porta a FC-VI	4	-
	Porta FC-VI b	-	4
	Porta FC-VI c	5	-
	Porta d. FC-VI	-	5
	HBA porta a	6	-
	Porta HBA b	-	6
	Porta HBA c	7	-
	Porta d. HBA	-	7

A tabela a seguir mostra o cabeamento do segundo grupo de DR:

		Brocade 6510		Brocade 6520		Brocade G620	
Componente	**Porto**	**Switch 1**	**Switch 2**	**Switch 1**	**Switch 2**	**Switch 1**	**Switch 2**

controller_x_3	Porta a FC-VI	24	-	48	-	18	-
	Porta FC-VI b	-	24	-	48	-	18
	Porta FC-VI c	25	-	49	-	19	-
	Porta d. FC-VI	-	25	-	49	-	19
	HBA porta a	26	-	50	-	24	-
	Porta HBA b	-	26	-	50	-	24
	Porta HBA c	27	-	51	-	25	-
	Porta d. HBA	-	27	-	51	-	25
controller_x_4	Porta a FC-VI	28	-	52	-	22	-
	Porta FC-VI b	-	28	-	52	-	22
	Porta FC-VI c	29	-	53	-	23	-
	Porta d. FC-VI	-	29	-	53	-	23
	HBA porta a	30	-	54	-	28	-
	Porta HBA b	-	30	-	54	-	28
	Porta HBA c	31	-	55	-	29	-
	Porta d. HBA	-	31	-	55	-	29
ISLs							
ISL 1	40	40	23	23	40	40	ISL 2
41	41	47	47	41	41	ISL 3	42

42	71	71	42	42	ISL 4	43	43
44	44	ISL 6	45	45	45		
45	ISL 7	46	46	46	46		

Uso de porta Cisco para controladores em uma configuração MetroCluster executando o ONTAP 9.4 ou posterior

As tabelas mostram a configuração máxima suportada, com oito módulos de controlador em dois grupos de DR. Para configurações menores, ignore as linhas dos módulos adicionais do controlador.

Utilização da porta Cisco 9396S

Cisco 9396S			
Componente	**Porto**	**Switch 1**	**Switch 2**
controller_x_1	Porta a FC-VI	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta d. FC-VI	-	2
	HBA porta a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta d. HBA	-	4

controller_x_2	Porta a FC-VI	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta d. FC-VI	-	6
	HBA porta a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta d. HBA	-	8
controller_x_3	Porta a FC-VI	49	
	Porta FC-VI b	-	49
	Porta FC-VI c	50	
	Porta d. FC-VI	-	50
	HBA porta a	51	
	Porta HBA b	-	51
	Porta HBA c	52	
	Porta d. HBA	-	52

controller_x_4	Porta a FC-VI	53	-
	Porta FC-VI b	-	53
	Porta FC-VI c	54	-
	Porta d. FC-VI	-	54
	HBA porta a	55	-
	Porta HBA b	-	55
	Porta HBA c	56	-
	Porta d. HBA	-	56

Utilização da porta Cisco 9148S

Cisco 9148S			
Componente	**Porto**	**Switch 1**	**Switch 2**
controller_x_1	Porta a FC-VI	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta d. FC-VI	-	2
	HBA porta a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta d. HBA	-	4

controller_x_2	Porta a FC-VI	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta d. FC-VI	-	6
	HBA porta a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta d. HBA	-	8
controller_x_3	Porta a FC-VI	25	
	Porta FC-VI b	-	25
	Porta FC-VI c	26	-
	Porta d. FC-VI	-	26
	HBA porta a	27	-
	Porta HBA b	-	27
	Porta HBA c	28	-
	Porta d. HBA	-	28

controller_x_4	Porta a FC-VI	29	-
	Porta FC-VI b	-	29
	Porta FC-VI c	30	-
	Porta d. FC-VI	-	30
	HBA porta a	31	-
	Porta HBA b	-	31
	Porta HBA c	32	-
	Porta d. HBA	-	32

Utilização da porta Cisco 9132T

Cisco 9132T			
Módulo MDS 1			
Componente	**Porto**	**Switch 1**	**Switch 2**
controller_x_1	Porta a FC-VI	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta d. FC-VI	-	2
	HBA porta a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta d. HBA	-	4

controller_x_2	Porta a FC-VI	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta d. FC-VI	-	6
	HBA porta a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta d. HBA	-	8
Módulo MDS 2			
Componente	**Porto**	**Switch 1**	**Switch 2**
controller_x_3	Porta a FC-VI	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta d. FC-VI	-	2
	HBA porta a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta d. HBA	-	4

controller_x_4	Porta a FC-VI	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta d. FC-VI	-	6
	HBA porta a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta d. HBA	-	8

Utilização da porta Cisco 9250

A tabela a seguir mostra sistemas com duas portas FC-VI. Os sistemas AFF A700 e FAS9000 têm quatro portas FC-VI (a, b, c e d). Se estiver usando um sistema AFF A700 ou FAS9000, as atribuições de portas se movem em uma posição. Por exemplo, as portas FC-VI c e d vão para a porta do switch 2 e as portas HBA a e b vão para a porta do switch 3.

Cisco 9250i			
O switch Cisco 9250i não é compatível com configurações MetroCluster de oito nós.			
Componente	**Porto**	**Switch 1**	**Switch 2**
controller_x_1	Porta a FC-VI	1	-
	Porta FC-VI b	-	1
	HBA porta a	2	-
	Porta HBA b	-	2
	Porta HBA c	3	-
	Porta d. HBA	-	3

controller_x_2	Porta a FC-VI	4	-
	Porta FC-VI b	-	4
	HBA porta a	5	-
	Porta HBA b	-	5
	Porta HBA c	6	-
	Porta d. HBA	-	6
controller_x_3	Porta a FC-VI	7	-
	Porta FC-VI b	-	7
	HBA porta a	8	-
	Porta HBA b	-	8
	Porta HBA c	9	-
	Porta d. HBA	-	9
controller_x_4	Porta a FC-VI	10	-
	Porta FC-VI b	-	10
	HBA porta a	11	-
	Porta HBA b	-	11
	Porta HBA c	13	-
	Porta d. HBA	-	13

Suporte a iniciador compartilhado e destino compartilhado para configuração MetroCluster com LUNs de array

Ser capaz de compartilhar uma determinada porta do iniciador de FC ou portas de destino é útil para organizações que desejam minimizar o número de portas do iniciador ou de destino usadas. Por exemplo, uma organização que espera baixo uso de e/S em uma porta de iniciador FC ou portas de destino pode preferir compartilhar porta de iniciador FC ou portas de destino em vez de dedicar cada porta de iniciador FC a uma única porta de destino.

No entanto, o compartilhamento de portas de iniciador ou destino pode afetar negativamente o desempenho.

"Como dar suporte à configuração Iniciador compartilhado e destino compartilhado com LUNs de array em um

ambiente MetroCluster"

Faça o cabeamento das portas FC-VI e HBA em uma configuração MetroCluster com LUNs de array

Fazer o cabeamento das portas FC-VI e HBA em uma configuração de MetroCluster conectada à malha de dois nós com LUNs de array

Se você estiver configurando uma configuração de MetroCluster conectada à malha de dois nós com LUNs de array, será necessário enviar por cabo as portas FC-VI e as portas HBA às portas do switch.

Sobre esta tarefa

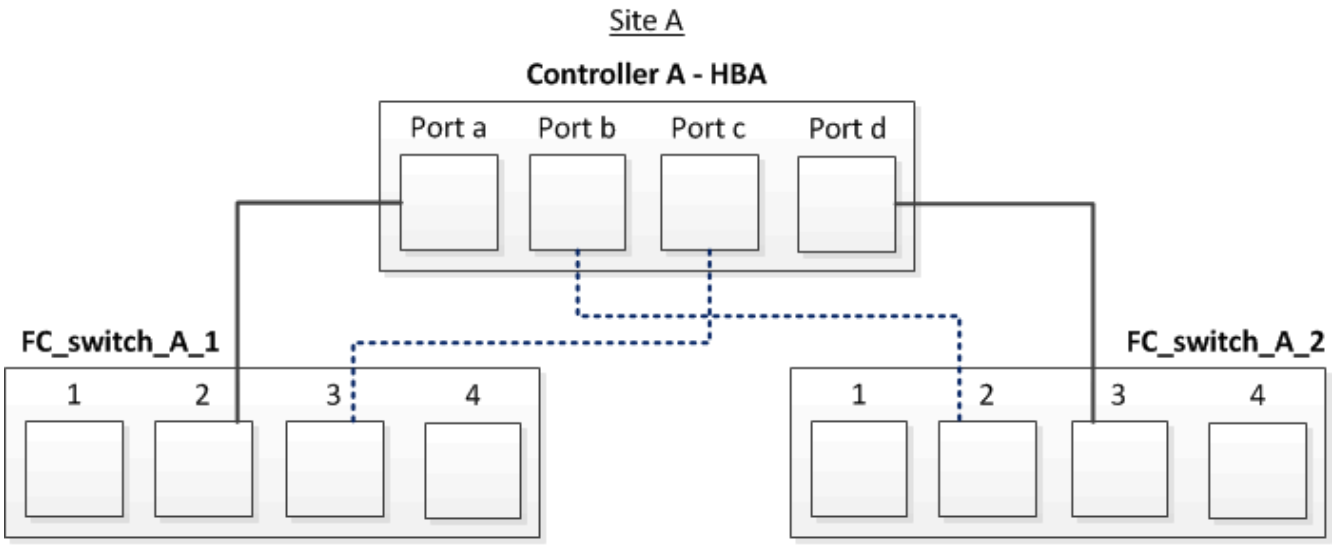
- Você deve repetir esta tarefa para cada controlador em ambos os sites do MetroCluster.
- Se você planeja usar discos além de LUNs de storage na configuração do MetroCluster, use as portas HBA e as portas de switch especificadas para configuração com discos.
  - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passos

1. Faça o cabeamento das portas FC-VI da controladora para as portas de switch alternativas.
2. Execute o cabeamento de controlador para switch em ambos os locais do MetroCluster.

   Você deve garantir redundância nas conexões do controlador para os switches. Portanto, para cada controlador em um local, você deve garantir que ambas as portas HBA no mesmo par de portas estejam conetadas a switches FC alternativos.

   O exemplo a seguir mostra as conexões entre as portas HBA no controlador A e as portas em FC_switch_A_1 e FC_switch_A_2:



   A tabela a seguir lista as conexões entre as portas HBA e as portas do switch FC na ilustração:

Portas HBA	Portas do switch
Par de portas	
Porta a	FC_switch_A_1, porta 2

Porta d	FC_switch_A_2, porta 3
Par de portas	
Porto b	FC_switch_A_2, porta 2
Porta c	FC_switch_A_1, porta 3

Depois de terminar

Você deve fazer o cabeamento das ISLs entre os switches FC nos locais do MetroCluster.

Fazer o cabeamento das portas FC-VI e HBA em uma configuração de MetroCluster conectada à malha de quatro nós com LUNs de array

Se você estiver configurando uma configuração MetroCluster conectada à malha de quatro nós com LUNs de array, será necessário enviar por cabo as portas FC-VI e as portas HBA às portas do switch.

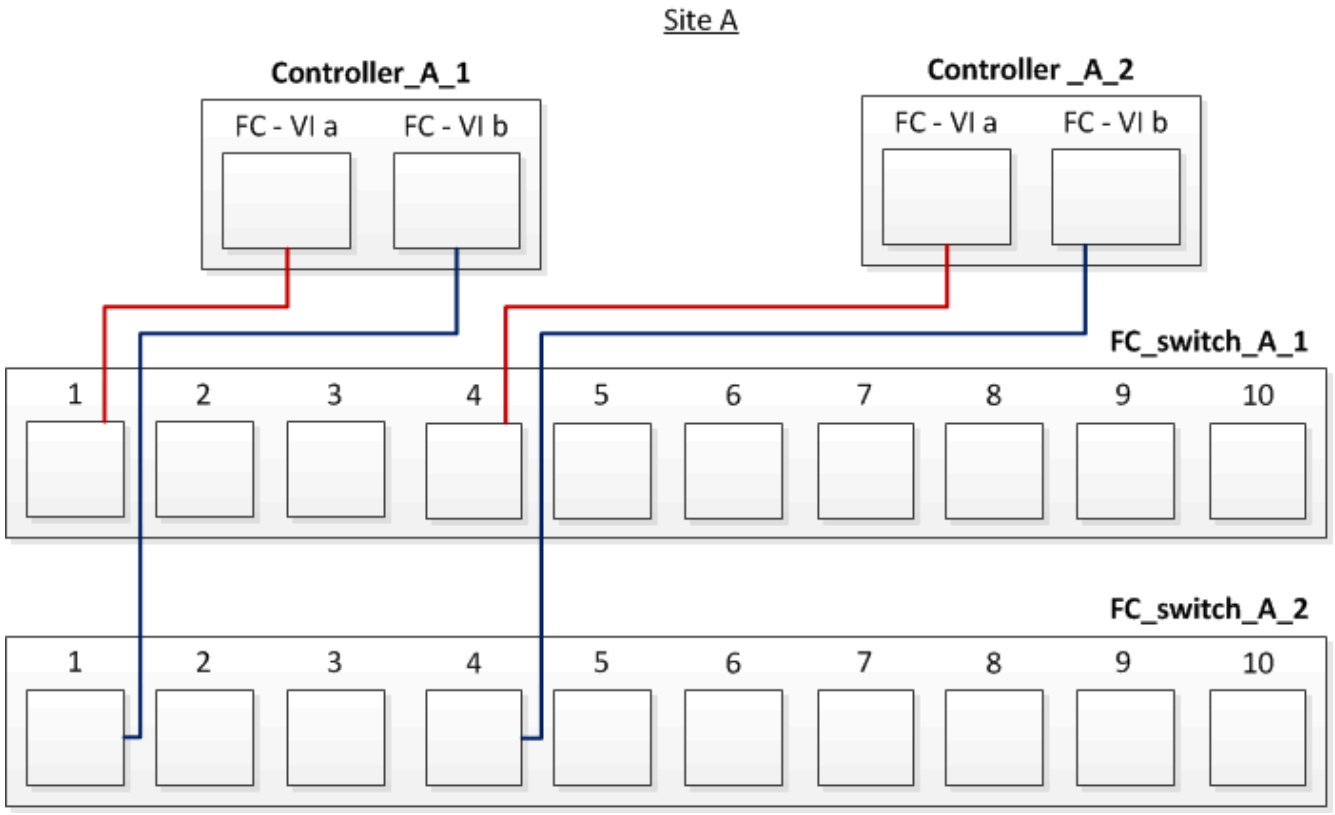
Sobre esta tarefa

- Você deve repetir esta tarefa para cada controlador em ambos os sites do MetroCluster.
- Se você planeja usar discos além de LUNs de storage na configuração do MetroCluster, use as portas HBA e as portas de switch especificadas para configuração com discos.
  - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passos

1. Faça o cabeamento das portas FC-VI de cada controlador para as portas em switches FC alternativos.

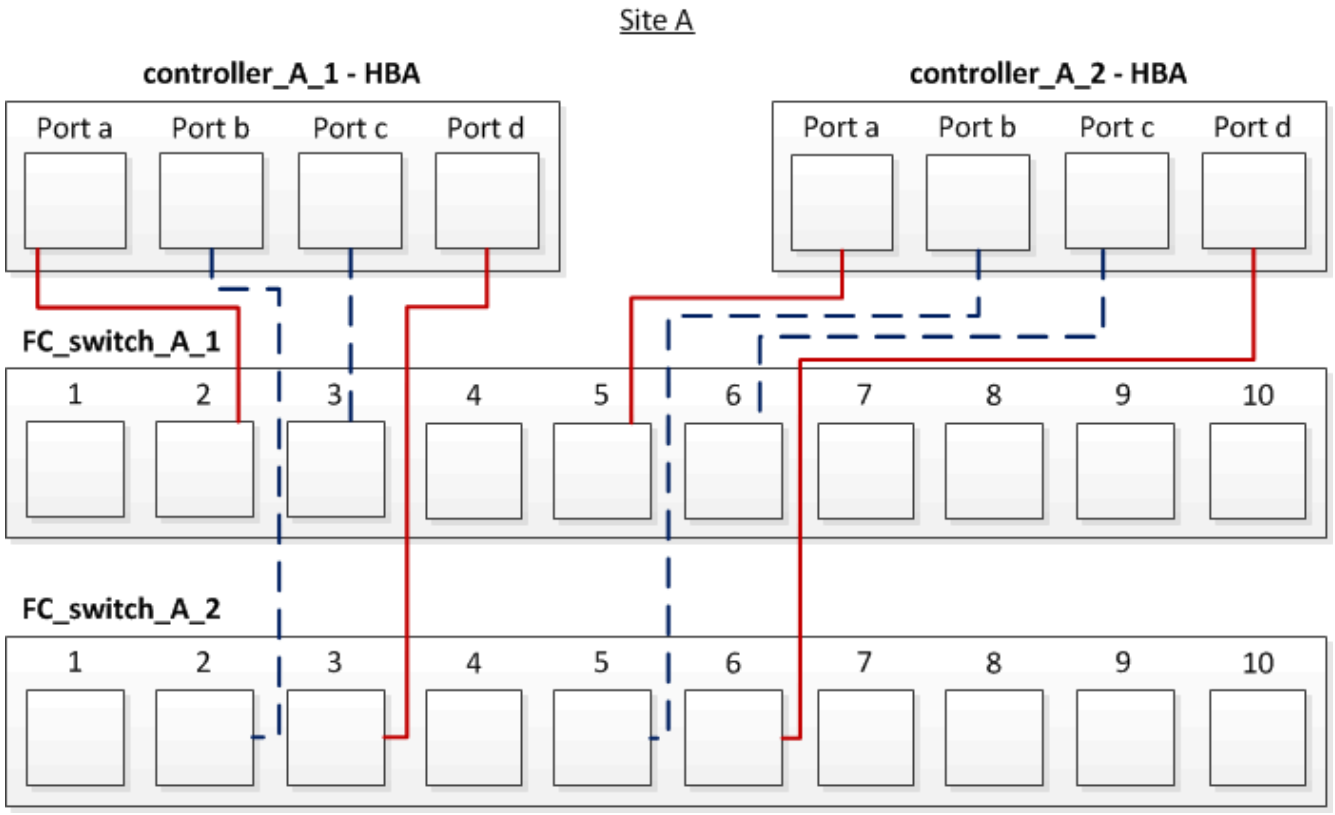
   O exemplo a seguir mostra as conexões entre as portas FC-VI e as portas do switch no local A:



2. Execute o cabeamento de controlador para switch em ambos os locais do MetroCluster.

   Você deve garantir redundância nas conexões do controlador para os switches. Portanto, para cada controlador em um local, você deve garantir que ambas as portas HBA no mesmo par de portas estejam conetadas a switches FC alternativos.

   O exemplo a seguir mostra as conexões entre as portas HBA e as portas do switch no local A:



A tabela a seguir lista as conexões entre as portas HBA em controller_A_1 e as portas do switch FC na ilustração:

Portas HBA	Portas do switch
Par de portas	
Porta a	FC_switch_A_1, porta 2
Porta d	FC_switch_A_2, porta 3
Par de portas	
Porto b	FC_switch_A_2, porta 2
Porta c	FC_switch_A_1, porta 3

A tabela a seguir lista as conexões entre as portas HBA em controller_A_2 e as portas do switch FC na ilustração:

Portas HBA	Portas do switch
Par de portas	
Porta a	FC_switch_A_1, porta 5
Porta d	FC_switch_A_2, porta 6

Par de portas	
Porto b	FC_switch_A_2, porta 5
Porta c	FC_switch_A_1, porta 6

Depois de terminar

Você deve fazer o cabeamento das ISLs entre os switches FC nos locais do MetroCluster.

Informações relacionadas

Quando você conecta sistemas ONTAP a switches FC para configurar uma configuração MetroCluster com LUNs de array, é necessário conectar portas FC-VI e HBA de cada controladora a portas de switch específicas.

"Portas de switch necessárias para uma configuração MetroCluster com LUNs de array"

Fazer o cabeamento das portas FC-VI e HBA em uma configuração de MetroCluster conectada à malha de oito nós com LUNs de array

Se você estiver configurando uma configuração MetroCluster conectada à malha de oito nós com LUNs de array, será necessário enviar por cabo as portas FC-VI e as portas HBA às portas do switch.

Sobre esta tarefa

- Você deve repetir esta tarefa para cada controlador em ambos os sites do MetroCluster.
- Se você planeja usar discos além de LUNs de storage na configuração do MetroCluster, use as portas HBA e as portas de switch especificadas para configuração com discos.
  - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passo

1. Cable as portas FC-VI e as portas HBA de cada controlador para as portas em switches FC alternativos. Consulte as seguintes tabelas:

Configurações de cabeamento para FibreBridge 7500N ou 7600N usando ambas as portas FC

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)					
MetroCluster 1 ou Grupo de RD 1					
Componente		Porta	Interrutor Brocade modelos 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 e DCX 8510-8		Interrutor Brocade G720
			Liga ao FC_switch…	Liga à porta do switch…	Liga à porta do switch…
controller_x_1	Porta a FC-VI	1	0	0	Porta FC-VI b
2	0	0	Porta FC-VI c	1	1

1	Porta d. FC-VI	2	1	1	HBA porta a
1	2	8	Porta HBA b	2	2
8	Porta HBA c	1	3	9	Porta d. HBA
2	3	9	controller_x_2	Porta a FC-VI	1
4	4	Porta FC-VI b	2	4	4
Porta FC-VI c	1	5	5	Porta d. FC-VI	2
5	5	HBA porta a	1	6	12
Porta HBA b	2	6	12	Porta HBA c	1
7	13	Porta d. HBA	2	7	13
Pilha 1	bridge_x_1a	FC1	1	8	10
	FC2	2	8	10	bridge_x_1B
	FC1	1	9	11	FC2
	2	9	11	Pilha 2	bridge_x_2a
FC1	1	10	14	FC2	2
10	14	bridge_x_2B	FC1	1	11
15	FC2	2	11	15	Pilha 3
bridge_x_3a	FC1	1	12*	16	FC2
2	12*	16	bridge_x_3B	FC1	1
13*	17	FC2	2	13*	17
Empilha y	bridge_x_ya	FC1	1	14*	20
FC2	2	14*	20	ponte_x_yb	FC1
1	15*	21	FC2	2	15*

Nota: As pontes adicionais podem ser cabeadas para as portas 16, 17, 20 e 21 nos switches G620, G630, G620-1 e G630-1.

Depois de terminar

Você deve fazer o cabeamento das ISLs entre os switches FC nos locais do MetroCluster.

Configurações de cabeamento do Cisco 9250i

Cisco 9250i*			
Componente	Porta	Interrutor 1	Interrutor 2
controller_x_1	Porta a FC-VI	1	-
Porta FC-VI b	-	1	HBA porta a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta d. HBA	-	3	controller_x_2
Porta a FC-VI	4	-	Porta FC-VI b
-	4	HBA porta a	5
-	Porta HBA b	-	5
Porta HBA c	6	-	Porta d. HBA
-	6	controller_x_3	Porta a FC-VI
7	-	Porta FC-VI b	-
7	HBA porta a	8	-
Porta HBA b	-	8	Porta HBA c
9	-	Porta d. HBA	-
9	controller_x_4	Porta a FC-VI	10
-	Porta FC-VI b	-	10
HBA porta a	11	-	Porta HBA b

-	11	Porta HBA c	13
-	Porta d. HBA	-	13

Depois de terminar

Você deve fazer o cabeamento das ISLs entre os switches FC nos locais do MetroCluster.

Cabeamento dos ISLs em uma configuração MetroCluster com LUNs de array

É necessário conectar os switches FC nos locais por meio de ISLs (Inter-Switch Links) para formar malhas de switch na configuração do MetroCluster com LUNs de array.

Passos

1. Conete os switches em cada local ao ISL ou ISLs, usando o cabeamento na tabela que corresponde à sua configuração e modelo de switch.

   Os números da porta do switch que você pode usar para os ISLs FC são os seguintes:

Modelo do interrutor	Porta de ISL	Porta do switch
Brocade 6520	Porta ISL 1	23
Porta ISL 2	47	Porta ISL 3
71	Porta ISL 4	95
Brocade 6505	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46
Porta ISL 8	47	Brocade 7810
Porta ISL 1	GE2 Gbps (10 Gbps)	Porta ISL 2

ge3 Gbps (10 Gbps)	Porta ISL 3	ge4 Gbps (10 Gbps)
Porta ISL 4	ge5 Gbps (10 Gbps)	Porta ISL 5
GE6 Gbps (10 Gbps)	Porta ISL 6	ge7 Gbps (10 Gbps)
Brocade 7840 **Nota**: O switch Brocade 7840 suporta duas portas VE de 40 Gbps ou até quatro portas VE de 10 Gbps por switch para a criação de ISLs FCIP.	Porta ISL 1	ge0 Gbps (40 Gbps) ou GE2 Gbps (10 Gbps)
Porta ISL 2	ge1 Gbps (40 Gbps) ou ge3 Gbps (10 Gbps)	Porta ISL 3
ge10 Gbps (10 Gbps)	Porta ISL 4	ge11 Gbps (10 Gbps)
Brocade G610	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
Brocade G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46
Modo de comutação l	Porta de ISL	Porta do switch
Cisco 9396S	ISL 1	44
	ISL 2	48
	ISL 3	92
	ISL 4	96

Cisco 9250i com licença de 24 portas	ISL 1	12
ISL 2	16	ISL 3
20	ISL 4	24
Cisco 9148S	ISL 1	20
ISL 2	24	ISL 3
44	ISL 4	48
Cisco 9132T	ISL 1	Módulo MDS 1 porta 13
	ISL 2	Módulo MDS 1 porta 14
	ISL 3	Módulo MDS 1 porta 15
	ISL 4	Módulo MDS 1 porta 16
* O switch Cisco 9250i usa as portas FCIP para o ISL. Existem certas limitações e procedimentos para o uso das portas FCIP.		
As portas 40 a 48 são portas de 10 GbE e não são usadas na configuração do MetroCluster.		

Cabeamento da interconexão de cluster em configurações de oito ou quatro nós

Em configurações de MetroCluster de oito ou quatro nós, você deve fazer o cabeamento da interconexão de cluster entre os módulos de controladora local em cada local.

Sobre esta tarefa

Esta tarefa não é necessária em configurações de MetroCluster de dois nós.

Esta tarefa deve ser executada em ambos os locais do MetroCluster.

Passo

1. Faça a interconexão de cluster de um módulo de controladora para o outro, ou se forem usados switches de interconexão de cluster, de cada módulo de controladora para os switches.

Informações relacionadas

"Documentação dos sistemas de hardware da ONTAP"

"Gerenciamento de rede e LIF"

Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de

cluster para que elas tenham conetividade com o cluster no site do parceiro.

Sobre esta tarefa

Esta tarefa deve ser executada em cada módulo do controlador na configuração do MetroCluster.

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

Passo

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

   O peering de cluster pode ser feito em portas dedicadas ou em portas de dados. O uso de portas dedicadas fornece maior taxa de transferência para o tráfego de peering de cluster.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

Cada site do MetroCluster é configurado como um ponto do site do parceiro. Você deve estar familiarizado com os pré-requisitos e diretrizes para configurar os relacionamentos de peering e ao decidir se usar portas compartilhadas ou dedicadas para esses relacionamentos.

"Peering de clusters"

Cabeamento da interconexão de HA

Se você tiver uma configuração de MetroCluster de oito ou quatro nós e os controladores de storage nos pares de HA estiverem em chassi separado, será necessário fazer o cabeamento da interconexão de HA entre as controladoras.

Sobre esta tarefa

- Esta tarefa não se aplica a configurações de MetroCluster de dois nós.
- Esta tarefa deve ser executada em ambos os locais do MetroCluster.
- A interconexão de HA só deve ser cabeada se as controladoras de storage dentro do par de HA estiverem em chassi separado.

  Alguns modelos de controladora de storage oferecem suporte a duas controladoras em um único chassi. Nesse caso, elas usam uma interconexão interna de HA.

Passos

1. Cable a interconexão de HA se o parceiro de HA da controladora de storage estiver em um chassi separado.

   "Documentação dos sistemas de hardware da ONTAP"

2. Se o local do MetroCluster incluir dois pares de HA, repita as etapas anteriores no segundo par de HA.
3. Repita esta tarefa no site do parceiro MetroCluster.

Cabeamento das conexões de dados e gerenciamento

Você deve encaminhar as portas de gerenciamento e dados em cada controlador de storage para as redes do local.

Sobre esta tarefa

Esta tarefa deve ser repetida para cada novo controlador em ambos os locais do MetroCluster.

Você pode conetar as portas de gerenciamento do controlador e do switch de cluster a switches existentes na rede ou a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passo

1. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

   "Documentação dos sistemas de hardware da ONTAP"

Storage arrays de cabo para switches FC em uma configuração MetroCluster

Cabeamento de storage arrays para switches FC em uma configuração MetroCluster

É necessário conectar storage arrays a switches FC para que os sistemas ONTAP na configuração MetroCluster possam acessar um LUN de array específico por pelo menos dois caminhos.

Antes de começar

- Os storage arrays devem ser configurados para apresentar LUNs de array ao ONTAP.
- Os controladores ONTAP devem ser conectados aos switches FC.
- Os ISLs devem ser cabeados entre os switches FC nos locais do MetroCluster.
- Você deve repetir essa tarefa para cada storage array em ambos os sites do MetroCluster.
- É necessário conectar os controladores em uma configuração MetroCluster aos storage arrays por meio de switches FC.

Passos

1. Conecte as portas do storage array às portas do switch FC.

   Em cada local, conecte os pares de portas redundantes no storage array a switches FC em malhas alternativas. Isso fornece redundância nos caminhos para acessar os LUNs do array.

Informações relacionadas

- A configuração do zoneamento de switch permite definir quais LUNs de array podem ser visualizados por um sistema ONTAP específico na configuração do MetroCluster.

  "Zoneamento de switch em uma configuração MetroCluster com LUNs de array"

- Em uma configuração MetroCluster com LUNs de array, você precisa conectar as portas de storage array que formam um par de portas redundante a switches FC alternativos.

  "Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de dois nós"

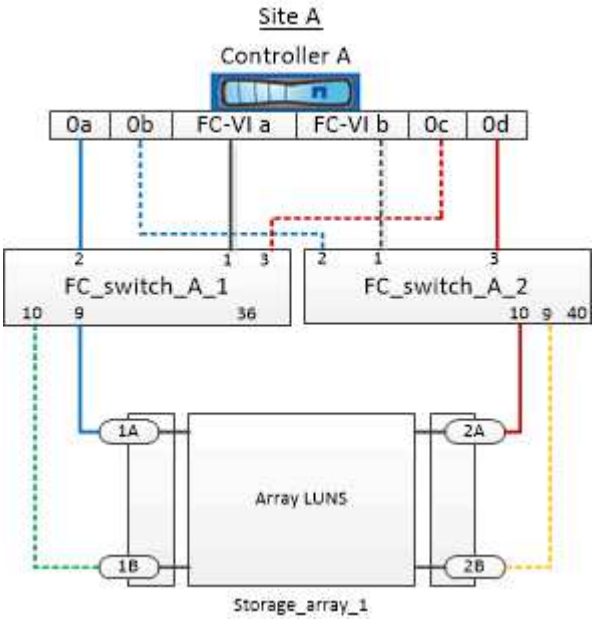
"Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de quatro nós"

"Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de oito nós"

Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de dois nós

Em uma configuração MetroCluster com LUNs de array, você precisa conectar as portas de storage array que formam um par de portas redundante a switches FC alternativos.

A ilustração a seguir mostra as conexões entre arrays de storage e switches FC em uma configuração de MetroCluster conetada à malha de dois nós com LUNs de storage:



As conexões entre portas de storage array e portas de switch FC são semelhantes para variantes alongadas e conetadas a malha de configurações de MetroCluster de dois nós com LUNs de array.

Se você planeja usar discos além dos LUNs de storage na configuração do MetroCluster, use as portas de switch especificadas para a configuração com discos.

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Na ilustração, os pares de portas de matriz redundantes para ambos os sites são os seguintes:

- Storage array no local A:
  - Portas 1A e 2A
  - Portas 1B e 2B
- Storage array no local B:
  - Portas 1A' e 2A'
  - Portas 1B' e 2B'

FC_switch_A_1 no local A e FC_switch_B_1 no local B estão conetados ao form Fabric_1. Da mesma forma, FC_switch_A_2 no local A e FC_switch_B_2 estão conetados ao form Fabric_2.

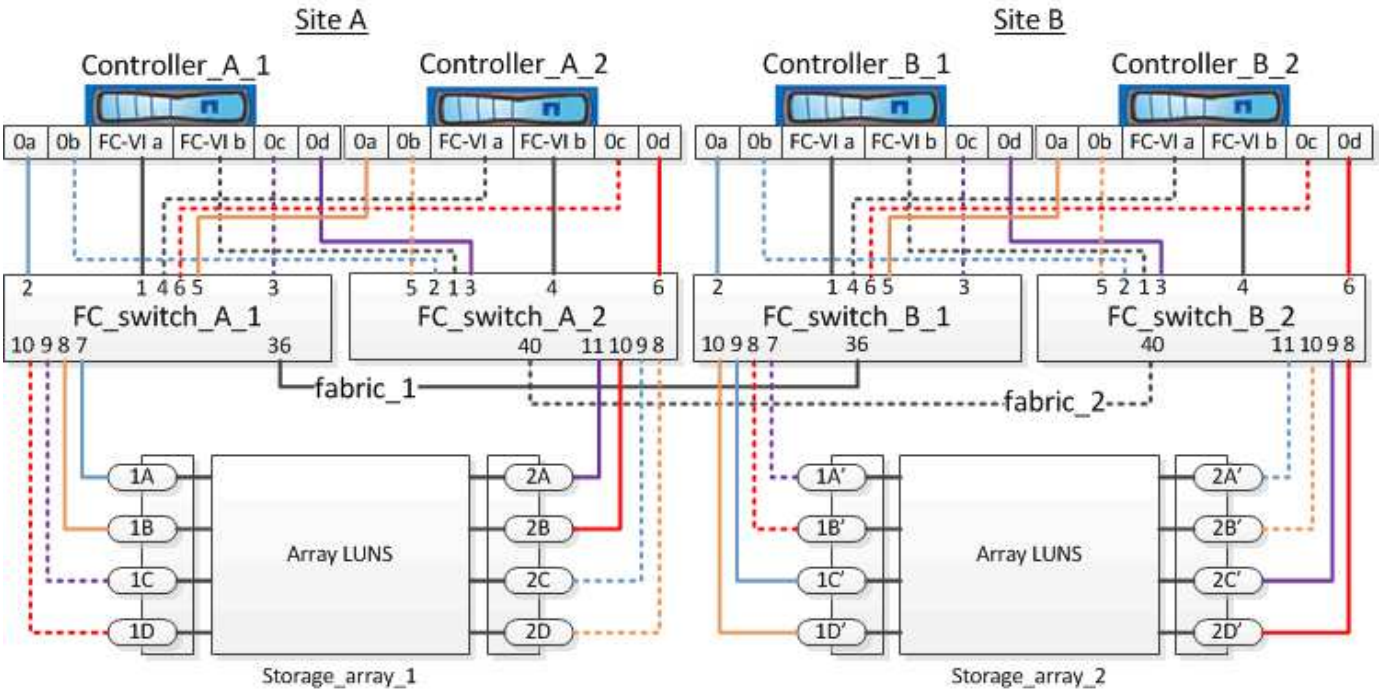
A tabela a seguir lista as conexões entre as portas do storage array e os switches FC para a ilustração MetroCluster de exemplo:

Portas LUN de array	Portas de switch FC	Troque de tecidos
Site A		
1A	FC_switch_A_1, porta 9	fabric_1
2A	FC_switch_A_2, porta 10	fabric_2
1B	FC_switch_A_1, porta 10	fabric_1
2B	FC_switch_A_2, porta 9	fabric_2
Site B		
1A'	FC_switch_B_1, porta 9	fabric_1
2A'	FC_switch_B_2, porta 10	fabric_2
1B'	FC_switch_B_1, porta 10	fabric_1
2B'	FC_switch_B_2, porta 9	fabric_2

Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de quatro nós

Em uma configuração MetroCluster com LUNs de array, você precisa conectar as portas de storage array que formam um par de portas redundante a switches FC alternativos.

A ilustração de referência a seguir mostra as conexões entre storage arrays e switches FC em uma configuração de MetroCluster de quatro nós com LUNs de array:



Se você planeja usar discos além dos LUNs de storage na configuração do MetroCluster, use as portas de switch especificadas para a configuração com discos.

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Na ilustração, os pares de portas de matriz redundantes para ambos os sites são os seguintes:

- Storage array no local A:
  - Portas 1A e 2A
  - Portas 1B e 2B
  - Portas 1C e 2C
  - Portas 1D e 2D
- Storage array no local B:
  - Portas 1A' e 2A'
  - Portas 1B' e 2B'
  - Portas 1C' e 2C'
  - Portas 1D' e 2D'

FC_switch_A_1 no local A e FC_switch_B_1 no local B estão conetados ao form Fabric_1. Da mesma forma, FC_switch_A_2 no local A e FC_switch_B_2 estão conetados ao form Fabric_2.

A tabela a seguir lista as conexões entre as portas do storage array e os switches FC para a ilustração MetroCluster:

Portas LUN de array	Portas de switch FC	Troque de tecidos
Site A		

1A	FC_switch_A_1, porta 7	fabric_1
2A	FC_switch_A_2, porta 11	fabric_2
1B	FC_switch_A_1, porta 8	fabric_1
2B	FC_switch_A_2, porta 10	fabric_2
1C	FC_switch_A_1, porta 9	fabric_1
2C	FC_switch_A_2, porta 9	fabric_2
1D	FC_switch_A_1, porta 10	fabric_1
2D	FC_switch_A_2, porta 8	fabric_2
Site B		
1A'	FC_switch_B_1, porta 7	fabric_1
2A'	FC_switch_B_2, porta 11	fabric_2
1B'	FC_switch_B_1, porta 8	fabric_1
2B'	FC_switch_B_2, porta 10	fabric_2
1C'	FC_switch_B_1, porta 9	fabric_1
2C'	FC_switch_B_2, porta 9	fabric_2
1D'	FC_switch_B_1, porta 10	fabric_1
2D'	FC_switch_B_2, porta 8	fabric_2

Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de oito nós

Em uma configuração MetroCluster com LUNs de array, você precisa conectar as portas de storage array que formam um par de portas redundante a switches FC alternativos.

Uma configuração do MetroCluster de oito nós consiste em dois grupos de DR de quatro nós. O primeiro grupo de DR consiste nos seguintes nós:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

O segundo grupo de DR consiste nos seguintes nós:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

Para fazer o cabeamento das portas do array para o primeiro grupo de DR, você pode usar os exemplos de cabeamento para uma configuração de MetroCluster de quatro nós para o primeiro grupo de DR.

"Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de quatro nós"

Para fazer o cabeamento das portas do array para o segundo grupo de DR, siga os mesmos exemplos e extrapolar para as portas FC-VI e portas iniciadores FC pertencentes às controladoras no segundo grupo de DR.

Zoneamento de switch em uma configuração MetroCluster com LUNs de array

Requisitos para zoneamento de switch em uma configuração MetroCluster com LUNs de array

Ao usar o zoneamento de switch em uma configuração do MetroCluster com LUNs de array, você deve garantir que certos requisitos básicos sejam seguidos.

Os requisitos para zoneamento de switch em uma configuração MetroCluster com LUNs de array são os seguintes:

- A configuração do MetroCluster deve seguir o esquema de zoneamento de um único iniciador para um único destino.

  O zoneamento de um único iniciador para um único destino limita cada zona a uma única porta de iniciador de FC e uma única porta de destino.

- As portas FC-VI precisam estar zoneadas de ponta a ponta em toda a malha.
- O compartilhamento de várias portas de iniciador com uma única porta de destino pode causar problemas de desempenho.

  Da mesma forma, o compartilhamento de várias portas de destino com uma única porta de iniciador pode causar problemas de desempenho.

- Você deve ter executado uma configuração básica dos switches FC usados na configuração do MetroCluster.
  - "Configure os switches Cisco FC manualmente"
  - "Configurar manualmente os switches Brocade FC"

Suporte a iniciador compartilhado e destino compartilhado para configuração MetroCluster com LUNs de array

Ser capaz de compartilhar uma determinada porta do iniciador de FC ou portas de destino é útil para organizações que desejam minimizar o número de portas do iniciador ou de destino usadas. Por exemplo, uma organização que espera baixo uso de e/S em uma porta de iniciador FC ou portas de destino pode preferir compartilhar porta de iniciador FC ou portas de destino em vez de dedicar cada porta de iniciador FC a uma única porta de destino.

No entanto, o compartilhamento de portas de iniciador ou destino pode afetar negativamente o desempenho.

Informações relacionadas

"Como dar suporte à configuração Iniciador compartilhado e destino compartilhado com LUNs de array em um ambiente MetroCluster"

- O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de dois nós com LUNs de array"

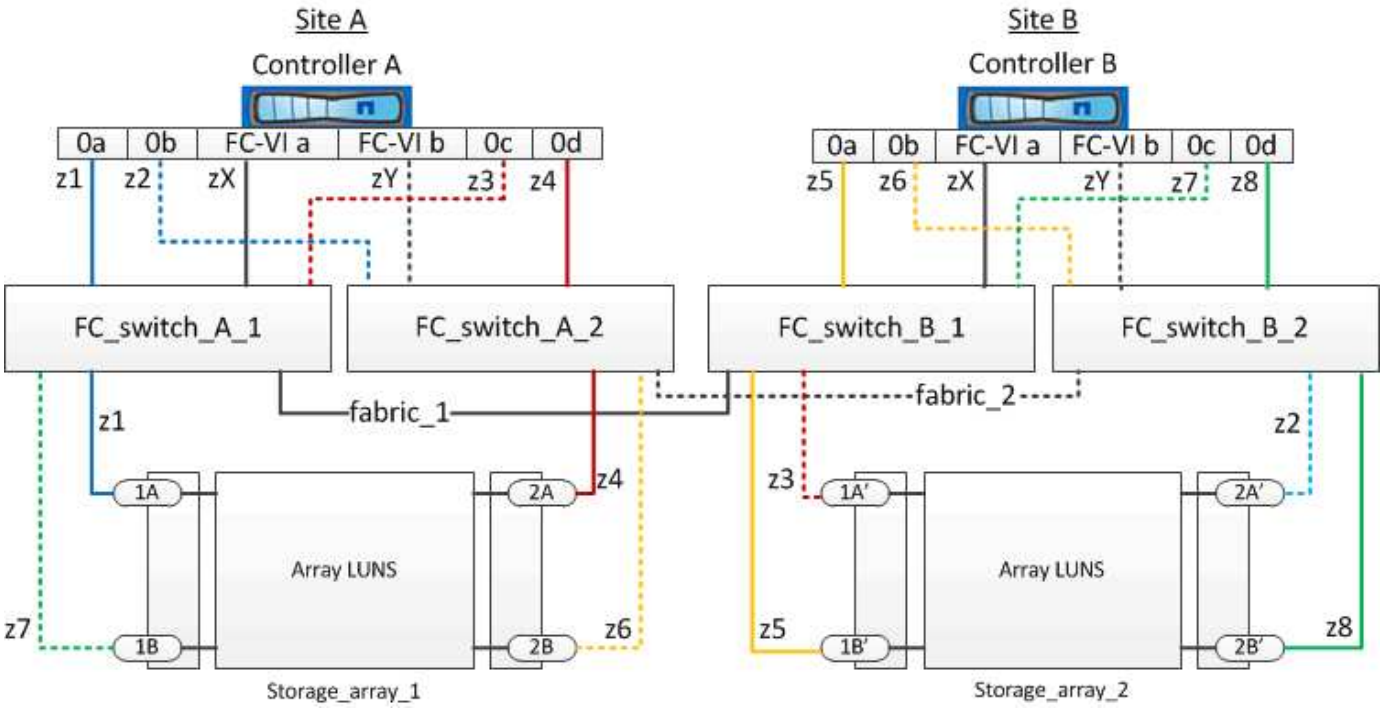
  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de oito nós com LUNs de array"

Exemplo de zoneamento de switch em uma configuração de MetroCluster de dois nós com LUNs de array

O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

Você pode usar o exemplo a seguir como referência ao determinar o zoneamento de uma configuração do MetroCluster conetada à malha de dois nós com LUNs de array:



O exemplo mostra o zoneamento de um único iniciador para um único destino para as configurações do MetroCluster. As linhas no exemplo representam zonas em vez de conexões; cada linha é rotulada com seu número de zona.

No exemplo, os LUNs de array são alocados em cada storage array. LUNs de igual tamanho são provisionados nos storage arrays de ambos os locais, o que é um requisito do SyncMirror. Cada sistema ONTAP tem dois caminhos para LUNs de array. As portas na matriz de armazenamento são redundantes.

Os pares de portas de matriz redundantes para ambos os sites são os seguintes:

- Storage array no local A:
  - Portas 1A e 2A
  - Portas 1B e 2B
- Storage array no local B:
  - Portas 1A' e 2A'
  - Portas 1B' e 2B'

Os pares de portas redundantes em cada storage array formam caminhos alternativos. Portanto, ambas as portas dos pares de portas podem acessar os LUNs nas respetivas matrizes de armazenamento.

A tabela a seguir mostra as zonas para as ilustrações:

Zona	Controlador ONTAP e porta do iniciador	Porta do array de storage
FC_switch_A_1		
z1	Controlador A: Porta 0a	Porta 1A
z3	Controlador A: Porta 0C	Porta 1A'
FC_switch_A_2		
z2	Controlador A: Porta 0b	Porta 2A'
z4	Controlador A: Porta 0d	Porta 2A
FC_switch_B_1		
z5	Controlador B: Porta 0a	Porta 1B'
z7	Controlador B: Porta 0C	Porta 1B
FC_switch_B_2		
z6	Controlador B: Porta 0b	Porta 2B
z8	Controlador B: Porta 0d	Porta 2B'

A tabela a seguir mostra as zonas para as conexões FC-VI:

Zona	Controlador ONTAP e porta do iniciador	Interrutor

Site A		
ZX	Controlador A: Porta FC-VI a	FC_switch_A_1
Zy	Controlador A: Porta FC-VI b	FC_switch_A_2
Site B		
ZX	Controlador B: Porta FC-VI a	FC_switch_B_1
Zy	Controlador B: Porta FC-VI b	FC_switch_B_2

Informações relacionadas

- O zoneamento do switch define caminhos entre nós conetados. Configurar o zoneamento permite definir quais LUNs de array podem ser visualizados por um sistema ONTAP específico.

  "Requisitos para zoneamento de switch em uma configuração MetroCluster com LUNs de array"

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"

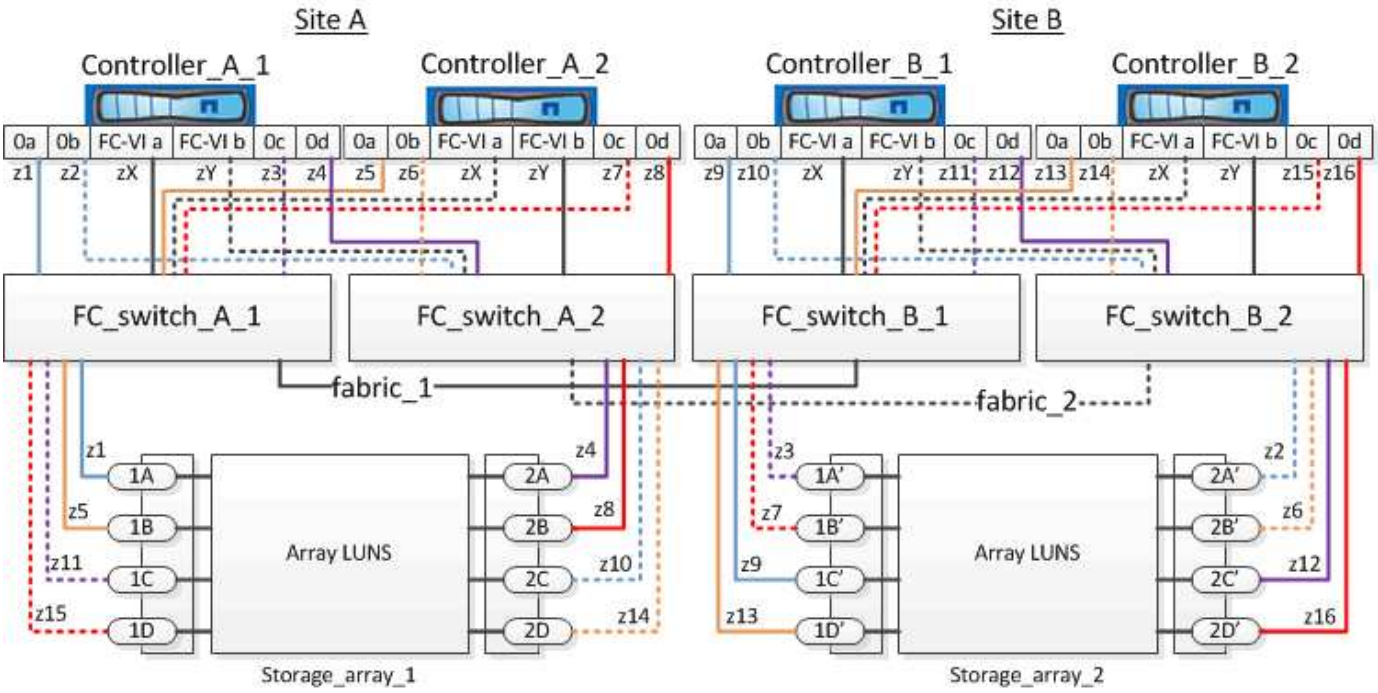
- Ao usar o zoneamento de switch em uma configuração do MetroCluster com LUNs de array, você deve garantir que certos requisitos básicos sejam seguidos.

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de oito nós com LUNs de array"

Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array

O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

Você pode usar o exemplo a seguir como referência ao determinar zoneamento para uma configuração de MetroCluster de quatro nós com LUNs de array. O exemplo mostra um único iniciador para um zoneamento de destino único para uma configuração do MetroCluster. As linhas no exemplo a seguir representam zonas em vez de conexões; cada linha é rotulada com seu número de zona:



Na ilustração, os LUNs de array são alocados em cada storage array para a configuração do MetroCluster. LUNs de igual tamanho são provisionados nos storage arrays de ambos os locais, o que é um requisito do SyncMirror. Cada sistema ONTAP tem dois caminhos para LUNs de array. As portas na matriz de armazenamento são redundantes.

Na ilustração, os pares de portas de matriz redundantes para ambos os sites são os seguintes:

- Storage array no local A:
  - Portas 1A e 2A
  - Portas 1B e 2B
  - Portas 1C e 2C
  - Portas 1D e 2D
- Storage array no local B:
  - Portas 1A' e 2A'
  - Portas 1B' e 2B'
  - Portas 1C' e 2C'
  - Portas 1D' e 2D'

Os pares de portas redundantes em cada storage array formam caminhos alternativos. Portanto, ambas as portas dos pares de portas podem acessar os LUNs nas respetivas matrizes de armazenamento.

As tabelas a seguir mostram as zonas para este exemplo:

Zonas para FC_switch_A_1

Zona	Controlador ONTAP e porta do iniciador	Porta do array de storage

z1	Controller_A_1: Porta 0a	Porta 1A
z3	Controller_A_1: Porta 0C	Porta 1A'
z5	Controller_A_2: Porta 0a	Porta 1B
z7	Controller_A_2: Porta 0C	Porta 1B'

Zonas para FC_switch_A_2

Zona	Controlador ONTAP e porta do iniciador	Porta do array de storage
z2	Controller_A_1: Porta 0b	Porta 2A'
z4	Controller_A_1: Porta 0d	Porta 2A
z6	Controller_A_2: Porta 0b	Porta 2B'
z8	Controller_A_2: Porta 0d	Porta 2B

Zonas para FC_switch_B_1

Zona	Controlador ONTAP e porta do iniciador	Porta do array de storage
z9	Controller_B_1: Porta 0a	Porta 1C'
z11	Controller_B_1: Porta 0C	Porta 1C
z13	Controller_B_2: Porta 0a	Porta 1D'
z15	Controller_B_2: Porta 0C	Porta 1D

Zonas para FC_switch_B_2

Zona	Controlador ONTAP e porta do iniciador	Porta do array de storage
z10	Controller_B_1: Porta 0b	Porta 2C
z12	Controller_B_1: Porta 0d	Porta 2C'
z14	Controller_B_2: Porta 0b	Porta 2D
z16	Controller_B_2: Porta 0d	Porta 2D'

Zonas para as conexões FC-VI no local A

Zona	Controlador ONTAP e porta do iniciador FC	Interrutor
ZX	Controller_A_1: Porta FC-VI a	FC_switch_A_1
Zy	Controller_A_1: Porta FC-VI b	FC_switch_A_2
ZX	Controller_A_2: Porta FC-VI a	FC_switch_A_1
Zy	Controller_A_2: Porta FC-VI b	FC_switch_A_2

Zonas para as ligações FC-VI no local B.

Zona	Controlador ONTAP e porta do iniciador FC	Interrutor
ZX	Controller_B_1: Porta FC-VI a	FC_switch_B_1
Zy	Controller_B_1: Porta FC-VI b	FC_switch_B_2
ZX	Controller_B_2: Porta FC-VI a	FC_switch_B_1
Zy	Controller_B_2: Porta FC-VI b	FC_switch_B_2

Informações relacionadas

- O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de dois nós com LUNs de array"

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de oito nós com LUNs de array"

- Ao usar o zoneamento de switch em uma configuração do MetroCluster com LUNs de array, você deve garantir que certos requisitos básicos sejam seguidos.

  "Requisitos para zoneamento de switch em uma configuração MetroCluster com LUNs de array"

Exemplo de zoneamento de switch em uma configuração de MetroCluster de oito nós com LUNs de array

O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

Uma configuração do MetroCluster de oito nós consiste em dois grupos de DR de quatro nós. O primeiro grupo de DR consiste nos seguintes nós:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

O segundo grupo de DR consiste nos seguintes nós:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

Para configurar o zoneamento do switch, você pode usar os exemplos de zoneamento para uma configuração de MetroCluster de quatro nós para o primeiro grupo de DR.

"Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"

Para configurar o zoneamento para o segundo grupo de DR, siga os mesmos exemplos e requisitos para as portas de iniciador FC e LUNs de array pertencentes aos controladores no segundo grupo de DR.

Informações relacionadas

- O zoneamento do switch define caminhos entre nós conetados. A configuração do zoneamento permite definir quais LUNs de array podem ser visualizados por sistemas ONTAP específicos.

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de dois nós com LUNs de array"

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"

- Ao usar o zoneamento de switch em uma configuração do MetroCluster com LUNs de array, você deve garantir que certos requisitos básicos sejam seguidos.

  "Requisitos para zoneamento de switch em uma configuração MetroCluster com LUNs de array"

Configure o ONTAP em uma configuração MetroCluster com LUNs de array

Verificar e configurar o estado HA dos componentes no modo Manutenção

Ao configurar um sistema de storage em uma configuração do MetroCluster, você deve garantir que o estado de alta disponibilidade (HA) do módulo do controlador e dos componentes do chassi seja "mcc" ou "mcc-2n" para que esses componentes sejam inicializados corretamente.

Antes de começar

O sistema tem de estar no modo de manutenção.

Sobre esta tarefa

Esta tarefa não é necessária em sistemas recebidos de fábrica.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado de HA correto depende da configuração do MetroCluster.

Número de controladores na configuração MetroCluster	O estado HA para todos os componentes deve ser…
Configuração de FC MetroCluster de oito ou quatro nós	mcc
Configuração de FC MetroCluster de dois nós	mcc-2n
Configuração IP do MetroCluster	mccip

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA para o módulo do controlador:

Número de controladores na configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify controller mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify controller mcc-2n`
Configuração IP do MetroCluster	`ha-config modify controller mccip`

3. Se o estado do sistema apresentado do chassis não estiver correto, defina o estado HA para o chassis:

Número de controladores na configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify chassis mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify chassis mcc-2n`
Configuração IP do MetroCluster	`ha-config modify chassis mccip`

4. Inicialize o nó no ONTAP:

   `boot_ontap`

5. Repita estas etapas em cada nó na configuração do MetroCluster.

Configuração do ONTAP em um sistema que usa apenas LUNs de array

Se você quiser configurar o ONTAP para uso com LUNs de array, configure o agregado raiz e o volume raiz, reserve espaço para operações de diagnóstico e recuperação e configure o cluster.

Antes de começar

- O sistema ONTAP deve ser conetado ao storage array.
- O administrador do storage array deve ter criado LUNs e apresentado ao ONTAP.
- O administrador da matriz de armazenamento deve ter configurado a segurança LUN.

Sobre esta tarefa

Você deve configurar cada nó que deseja usar com LUNs de array. Se o nó estiver em um par de HA, será necessário concluir o processo de configuração em um nó antes de prosseguir com a configuração no nó do parceiro.

Passos

1. Ligue o nó principal e interrompa o processo de inicialização pressionando Ctrl-C quando você vir a seguinte mensagem no console:

   ```
   Press CTRL-C for special boot menu.
   ```

2. Selecionar a opção **4 (limpar configuração e inicializar todos os discos)** no menu de inicialização.

   É apresentada a lista de LUNs de array disponibilizados para o ONTAP. Além disso, o tamanho do LUN do array necessário para a criação do volume raiz também é especificado. O tamanho necessário para a criação de volume raiz difere de um sistema ONTAP para outro.

   - Se nenhum LUN de array foi atribuído anteriormente, o ONTAP deteta e exibe os LUNs de array disponíveis, como mostrado no exemplo a seguir:

```
mcc8040-ams1::> disk show  NET-1.6 -instance
                  Disk: NET-1.6
        Container Type: aggregate
            Owner/Home: mcc8040-ams1-01 / mcc8040-ams1-01
               DR Home: -
    Stack ID/Shelf/Bay: -  / -  / -
                   LUN: 0
                 Array: NETAPP_INF_1
                Vendor: NETAPP
                 Model: INF-01-00
         Serial Number: 60080E50004317B4000003B158E35974
                   UID:
60080E50:004317B4:000003B1:58E35974:00000000:00000000:00000000:000000
00:00000000:00000000
                   BPS: 512
         Physical Size: 87.50GB
              Position: data
Checksum Compatibility: block
             Aggregate: eseries
                  Plex: plex0
Paths:
                                LUN  Initiator Side        Target
Side                                                       Link
Controller         Initiator     ID  Switch Port           Switch
Port           Acc Use  Target Port                TPGN    Speed
I/O KB/s          IOPS
------------------ ---------  -----  --------------------
--------------------  --- ---  ----------------------  ------
-------  ------------  ------------
mcc8040-ams1-01    2c             0  mccb6505-ams1:16      mccb6505-
ams1:18      AO  INU  20330080e54317b4              1   4 Gb/S
0             0
mcc8040-ams1-01    2a             0  mccb6505-ams1:17      mccb6505-
ams1:19      ANO RDY  20320080e54317b4              0   4 Gb/S
0             0

Errors:
-
```

- Se os LUNs de storage tiverem sido atribuídos anteriormente, por exemplo, pelo modo de manutenção, eles serão marcados como locais ou parceiros na lista dos LUNs de storage disponíveis, dependendo se os LUNs de storage foram selecionados no nó no qual você está instalando o ONTAP ou seu parceiro de HA:

  Neste exemplo, LUNs de array com números de índice 3 e 6 são marcados como "local" porque tinham sido previamente atribuídos a partir deste nó específico:

```
*************************************************************************
* No disks are owned by this node, but array LUNs are assigned.      *
* You can use the following information to verify connectivity from  *
* HBAs to switch ports.  If the connectivity of HBAs to switch ports *
* does not match your expectations, configure your SAN and rescan.   *
* You can rescan by entering 'r' at the prompt for selecting         *
* array LUNs below.

*************************************************************************
             HBA  HBA WWPN           Switch port      Switch port WWPN
              ---  --------           -----------      ----------------
              0e 500a098001baf8e0  vgbr6510s203:25      20190027f88948dd
              0f 500a098101baf8e0 vgci9710s202:1-17
2011547feeead680
              0g 500a098201baf8e0  vgbr6510s203:27      201b0027f88948dd
              0h 500a098301baf8e0 vgci9710s202:1-18
2012547feeead680


No native disks were detected, but array LUNs were detected.
You will need to select an array LUN to be used to create the root
aggregate and root volume.

The array LUNs visible to the system are listed below.  Select one array
LUN to be used to
create the root aggregate and root volume.  **The root volume requires
350.0 GB of space.**

 Warning: The contents of the array LUN you select will be erased by
ONTAP prior to their use.

Index  Array LUN Name           Model   Vendor    Size    Owner
Checksum  Serial Number
-----  ----------------------  ------  ------  --------  ------
--------  ------------------------
   0   vgci9710s202:2-24.0L19   RAID5   DGC     217.3 GB          Block
6006016083402B0048E576D7
   1   vgbr6510s203:30.126L20   RAID5   DGC     217.3 GB          Block
6006016083402B0049E576D7
   2   vgci9710s202:2-24.0L21   RAID5   DGC     217.3 GB          Block
6006016083402B004AE576D7
   3   vgbr6510s203:30.126L22   RAID5   DGC     405.4 GB  local   Block
6006016083402B004BE576D7
   4   vgci9710s202:2-24.0L23   RAID5   DGC     217.3 GB          Block
6006016083402B004CE576D7
   5   vgbr6510s203:30.126L24   RAID5   DGC     217.3 GB          Block
```

```
6006016083402B004DE576D7
   6   vgbr6510s203:30.126L25   RAID5   DGC     423.5 GB  local   Block
6006016083402B003CF93694
   7   vgci9710s202:2-24.0L26   RAID5   DGC     423.5 GB          Block
6006016083402B003DF93694
```

3. Selecione o número de índice correspondente ao LUN de matriz que deseja atribuir como volume raiz.

   O LUN de array deve ser de tamanho suficiente para criar o volume raiz.

   O LUN de array selecionado para criação de volume raiz é marcado como "local (raiz)".

   No exemplo a seguir, o LUN de matriz com o número de índice 3 é marcado para a criação de volume raiz:

```
The root volume will be created on switch 0:5.183L33.

**ONTAP requires that 11.0 GB of space be reserved for use in diagnostic
and recovery
operations.**  Select one array LUN to be used as spare for diagnostic
and recovery operations.

Index Array LUN Name    Model       Vendor    Size   Owner
Checksum  Serial Number
----- ----------------- ----------  ------  -------- --------------
--------  ------------------------
   0  switch0:5.183L1   SYMMETRIX   EMC     266.1 GB
Block     600604803436313734316631
   1  switch0:5.183L3   SYMMETRIX   EMC     266.1 GB
Block     600604803436316333353837
   2  switch0:5.183L31  SYMMETRIX   EMC     266.1 GB
Block     600604803436313237643666
   3  switch0:5.183L33  SYMMETRIX   EMC     658.3 GB local  (root)
Block     600604803436316263613066
   4  switch0:7.183L0   SYMMETRIX   EMC     173.6 GB
Block     600604803436313261356235
   5  switch0:7.183L2   SYMMETRIX   EMC     173.6 GB
Block     600604803436313438396431
   6  switch0:7.183L4   SYMMETRIX   EMC     658.3 GB
Block     600604803436313161663031
   7  switch0:7.183L30  SYMMETRIX   EMC     173.6 GB
Block     600604803436316538353834
   8  switch0:7.183L32  SYMMETRIX   EMC     266.1 GB
Block     600604803436313237353738
   9  switch0:7.183L34  SYMMETRIX   EMC     658.3 GB
Block     600604803436313737333662
```

4. Selecione o número de índice correspondente ao LUN de matriz que deseja atribuir para uso nas opções de diagnóstico e recuperação.

   O LUN do array deve ser de tamanho suficiente para ser usado nas opções de diagnóstico e recuperação. Se necessário, você também pode selecionar vários LUNs de matriz com um tamanho combinado maior ou igual ao tamanho especificado. Para selecionar várias entradas, você deve inserir os valores separados por vírgulas de todos os números de índice correspondentes aos LUNs de matriz que deseja selecionar para opções de diagnóstico e recuperação.

   O exemplo a seguir mostra uma lista de LUNs de array selecionados para criação de volume raiz e para opções de diagnóstico e recuperação:

```
Here is a list of the selected array LUNs
Index Array LUN Name     Model      Vendor    Size    Owner
Checksum  Serial Number
----- -----------------  ---------  ------  --------  -------------
--------  ------------------------
   2  switch0:5.183L31   SYMMETRIX  EMC     266.1 GB  local
Block     60060480343631323764366 6
   3  switch0:5.183L33   SYMMETRIX  EMC     658.3 GB  local   (root)
Block     60060480343631626361306 6
   4  switch0:7.183L0    SYMMETRIX  EMC     173.6 GB  local
Block     60060480343631326135623 5
   5  switch0:7.183L2    SYMMETRIX  EMC     173.6 GB  local
Block     60060480343631343839643 1
Do you want to continue (yes|no)?
```

   Selecionar "'no'" limpa a seleção de LUN.

5. Digite **y** quando solicitado pelo sistema para continuar com o processo de instalação.

   O agregado raiz e o volume raiz são criados e o restante do processo de instalação continua.

6. Insira os detalhes necessários para criar a interface de gerenciamento de nós.

   O exemplo a seguir mostra a tela da interface de gerenciamento de nó com uma mensagem confirmando a criação da interface de gerenciamento de nó:

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
     Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

Enter the node management interface port [e0M]:
Enter the node management interface IP address: 192.0.2.66

Enter the node management interface netmask: 255.255.255.192
Enter the node management interface default gateway: 192.0.2.7
A node management interface on port e0M with IP address 192.0.2.66 has
been created.

This node has its management address assigned and is ready for cluster
setup.
```

Depois de terminar

Depois de configurar o ONTAP em todos os nós que você deseja usar com LUNs de array, você deve concluir o "Processo de configuração do cluster"

Informações relacionadas

"Referência e requisitos de instalação da virtualização do FlexArray"

Configurar o cluster

A configuração do cluster envolve a configuração de cada nó, a criação do cluster no primeiro nó e a junção de todos os nós restantes ao cluster.

Informações relacionadas

"Configuração do software"

Instalar a licença para o uso de LUNs de array em uma configuração MetroCluster

Você deve instalar a licença V_StorageAttach em cada nó MetroCluster que deseja usar com LUNs de array. Não é possível usar LUNs de array em um agregado até que a licença seja instalada.

Antes de começar

- O cluster deve ser instalado.
- Você deve ter a chave de licença para a licença V_StorageAttach.

Sobre esta tarefa

Você deve usar uma chave de licença separada para cada nó no qual deseja instalar a licença V_StorageAttach.

Passos

1. Instale a licença V_StorageAttach.

   `system license add`

   Repita esta etapa para cada nó de cluster no qual você deseja instalar a licença.

2. Verifique se a licença V_StorageAttach está instalada em todos os nós necessários em um cluster.

   `system license show`

   A saída de exemplo a seguir mostra que a licença V_StorageAttach está instalada nos nós de cluster_A:

```
cluster_A::> system license show
Serial Number: nnnnnnnn
Owner: controller_A_1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage


Serial Number: llllllll
Owner: controller_A_2
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage
```

Configurando portas FC-VI em uma placa quad-port X1132A-R6 em sistemas FAS8020

Se você estiver usando a placa quad-port X1132A-R6 em um sistema FAS8020, você pode entrar no modo de manutenção para configurar as portas 1a e 1b para uso de FC-VI e iniciador. Isso não é necessário nos sistemas MetroCluster recebidos de fábrica, nos quais as portas são definidas adequadamente para sua configuração.

Sobre esta tarefa

Esta tarefa deve ser executada no modo Manutenção.

> A conversão de uma porta FC para uma porta FC-VI com o `ucadmin` comando só é suportada nos sistemas FAS8020 e AFF 8020. A conversão de portas FC para portas FCVI não é compatível em nenhuma outra plataforma.

Passos

1. Desative as portas:

```
storage disable adapter 1a

storage disable adapter 1b
```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Verifique se as portas estão desativadas:

```
ucadmin show
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. Defina as portas a e b para o modo FC-VI:

```
ucadmin modify -adapter 1a -type fcvi
```

O comando define o modo em ambas as portas no par de portas, 1a e 1b (mesmo que apenas 1a seja especificado no comando).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. Confirme se a alteração está pendente:

   `ucadmin show`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Desligue o controlador e reinicie-o no modo de manutenção.
6. Confirme a alteração de configuração:

   `ucadmin show local`

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

Atribuição de propriedade de LUNs de array

Os LUNs de array devem ser de propriedade de um nó antes que possam ser adicionados a um agregado para ser usado como storage.

Antes de começar

- O teste de configuração de back-end (teste da conetividade e configuração dos dispositivos por trás dos sistemas ONTAP) deve ser concluído.
- Os LUNs de array que você deseja atribuir devem ser apresentados aos sistemas ONTAP.

Sobre esta tarefa

Você pode atribuir a propriedade de LUNs do array que têm as seguintes características:

- Eles são de propriedade própria.
- Eles não têm erros de configuração de storage array, como os seguintes:
  - O LUN de array é menor ou maior do que o tamanho que o ONTAP suporta.
  - O LDEV é mapeado em apenas uma porta.
  - O LDEV tem IDs LUN inconsistentes atribuídas a ele.
  - O LUN está disponível apenas em um caminho.

O ONTAP emite uma mensagem de erro se você tentar atribuir a propriedade de um LUN de array com erros de configuração de back-end que interfeririam com o sistema ONTAP e o storage array operando em conjunto. Você deve corrigir esses erros antes de prosseguir com a atribuição de LUN de matriz.

O ONTAP o alerta se você tentar atribuir um LUN de matriz com um erro de redundância: Por exemplo, todos os caminhos para esse LUN de matriz são conetados ao mesmo controlador ou apenas um caminho para o LUN de matriz. Você pode corrigir um erro de redundância antes ou depois de atribuir a propriedade do LUN.

Passos

1. Exibir os LUNs do array que ainda não foram atribuídos a um nó:

   ```
   storage disk show -container-type unassigned
   ```

2. Atribua um LUN de matriz a este nó:

   ```
   storage disk assign -disk array_LUN_name -owner nodename
   ```

   Se você quiser corrigir um erro de redundância após a atribuição de disco em vez de antes, você deve usar o `-force` parâmetro com o comando de atribuição de disco de armazenamento.

Informações relacionadas

"Referência e requisitos de instalação da virtualização do FlexArray"

Peering dos clusters

Os clusters na configuração do MetroCluster precisam estar em um relacionamento de mesmo nível para que possam se comunicar uns com os outros e executar o espelhamento de dados essencial para a recuperação de desastres do MetroCluster.

Passos

1. Configure LIFs entre clusters usando o procedimento em:

   "Configurando LIFs entre clusters"

2. Crie um relacionamento de pares de cluster usando o procedimento em:

   "Peering dos clusters"

Espelhamento dos agregados de raiz

Você precisa espelhar os agregados raiz em sua configuração do MetroCluster para garantir a proteção de dados.

Antes de começar

Você precisa garantir que os requisitos do SyncMirror para a configuração MetroCluster com LUNs de array sejam atendidos. "Requisitos para uma configuração MetroCluster com LUNs de array"Consulte a .

Sobre esta tarefa

Você deve repetir esta tarefa para cada controlador na configuração do MetroCluster.

Passo

1. Espelhar o agregado de raiz sem espelhamento:

   `storage aggregate mirror`

   O comando a seguir espelha o agregado raiz para controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   O agregado de raiz é espelhado com LUNs de array de pool1.

Criação de agregados de dados sobre, implementação e verificação da configuração do MetroCluster

Você precisa criar agregados de dados em cada nó, implementar e verificar a configuração do MetroCluster.

Passos

1. Crie agregados de dados em cada nó:
   a. Crie um agregado de dados espelhados em cada nó:

      "Espelhar os agregados de raiz".

   b. Se necessário, crie agregados de dados sem espelhamento:

      "Crie um agregado de dados espelhados em cada nó".

2. "Implementar a configuração do MetroCluster".
3. "Configurar os switches MetroCluster FC para monitoramento de integridade".
4. Verifique e verifique a configuração:

a. "Verifique a configuração do MetroCluster".
b. "Verifique se há erros de configuração do MetroCluster com o Config Advisor".
c. "Verifique o switchover, a recuperação e o switchback".

5. Instale e configure o software tiebreaker do MetroCluster:
   a. "Instale o software tiebreaker".
   b. "Configure o software tiebreaker".
6. Defina o destino dos ficheiros de cópia de segurança de configuração:

"Proteja os arquivos de backup de configuração".

Implementar uma configuração MetroCluster com discos e LUNs de array

Implementação de uma configuração MetroCluster com discos e LUNs de array

Para implementar uma configuração MetroCluster com discos nativos e LUNs de array, é necessário garantir que os sistemas ONTAP usados na configuração possam ser anexados a storage arrays.

Uma configuração MetroCluster com discos e LUNs de array pode ter dois ou quatro nós. Embora a configuração de MetroCluster de quatro nós precise ser conetada à malha, a configuração de dois nós pode ser alongada ou conectada à malha.

No "Ferramenta de Matriz de interoperabilidade NetApp (IMT)", você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

Informações relacionadas

Para configurar uma configuração de MetroCluster com conexão de malha de dois nós ou uma configuração de MetroCluster de quatro nós com discos nativos e LUNs de array, você precisa usar pontes FC para SAS para conectar os sistemas ONTAP com os compartimentos de disco por meio dos switches FC. É possível conectar LUNs de array por meio dos switches FC aos sistemas ONTAP.

"Exemplo de uma configuração de MetroCluster conectada à malha de dois nós com discos e LUNs de array"

"Exemplo de uma configuração de MetroCluster de quatro nós com discos e LUNs de array"

Considerações ao implementar uma configuração MetroCluster com discos e LUNs de array

Ao Planejar a configuração do MetroCluster para uso com discos e LUNs de array, você deve considerar vários fatores, como a ordem de configuração de acesso ao storage, a localização de agregado de raiz e a utilização de portas de iniciador FC, switches e pontes FC para SAS.

Considere as informações na tabela a seguir ao Planejar sua configuração:

Consideração	Diretriz

Ordem de configurar o acesso ao armazenamento	Você pode configurar primeiro o acesso a discos ou LUNs de array. Você deve concluir toda a configuração para esse tipo de armazenamento e verificar se ele está configurado corretamente antes de configurar o outro tipo de armazenamento.
Localização do agregado raiz	• Se você estiver configurando uma implantação *new* MetroCluster com discos e LUNs de array, será necessário criar o agregado raiz em discos nativos. Ao fazer isso, certifique-se de que *pelo menos um* compartimento de disco (com 24 unidades de disco) esteja configurado em cada um dos sites. • Se você estiver adicionando discos nativos a uma configuração *existente* MetroCluster que use LUNs de array, o agregado raiz poderá permanecer em um LUN de array.
Uso de switches e pontes FC para SAS	As pontes FC para SAS são necessárias em configurações de quatro nós e em configurações conectadas à malha de dois nós para conectar os sistemas ONTAP às gavetas de disco por meio dos switches. Você precisa usar os mesmos switches para se conectar aos storage arrays e às pontes FC para SAS.
Usando portas do iniciador FC	As portas do iniciador usadas para se conectar a uma ponte FC para SAS devem ser diferentes das portas usadas para conexão aos switches, que se conectam aos storage arrays. Um mínimo de oito portas de iniciador é necessário para conetar um sistema ONTAP a discos e LUNs de array.

Informações relacionadas

- Os procedimentos e comandos de configuração do switch são diferentes, dependendo do fornecedor do switch.

  "Configuração manual dos switches Brocade FC"

  "Configuração manual dos switches Cisco FC"

- Você instala e faz o cabeamento de pontes ATTO FibreBridge e gavetas de disco SAS ao adicionar novo armazenamento à configuração.

  "Instalação de pontes FC para SAS e gavetas de disco SAS"

- O zoneamento do switch define caminhos entre nós conetados. Configurar o zoneamento permite definir quais LUNs de array podem ser visualizados por um sistema ONTAP específico.

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"

  "Exemplo de zoneamento de switch em uma configuração de MetroCluster de oito nós com LUNs de array"

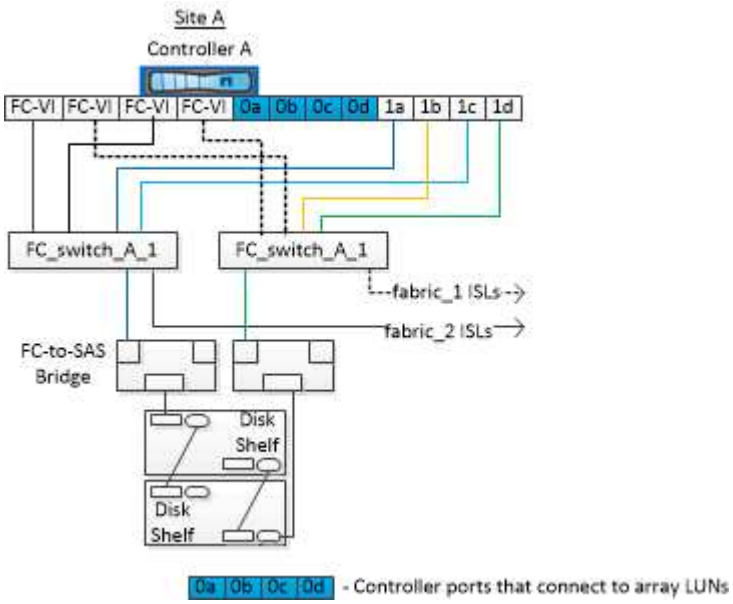
- "NetApp Hardware Universe"

Exemplo de uma configuração de MetroCluster conectada à malha de dois nós com discos e LUNs de array

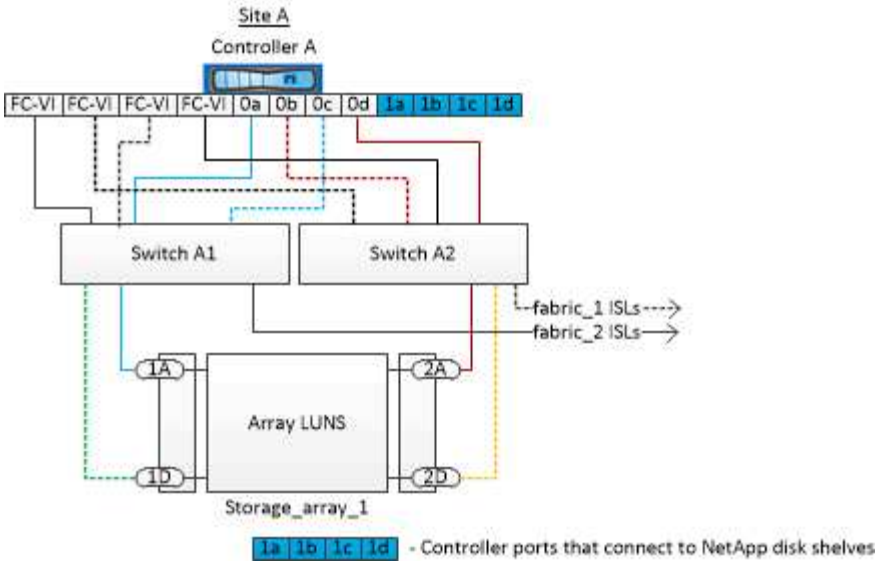
Para configurar uma configuração de MetroCluster com conexão de malha de dois nós com discos nativos e LUNs de array, é necessário usar pontes FC para SAS para conectar os sistemas ONTAP aos compartimentos de disco por meio dos switches FC. É possível conectar LUNs de array por meio dos switches FC aos sistemas ONTAP.

As ilustrações a seguir representam exemplos de uma configuração MetroCluster conectada à malha de dois nós com discos e LUNs de array. Ambas representam a mesma configuração MetroCluster; as representações para discos e LUNs de array são separadas apenas para simplificação.

Na ilustração a seguir mostrando a conectividade entre sistemas e discos ONTAP, as portas HBA 1a a 1D são usadas para conetividade com discos por meio das pontes FC-para-SAS:



Na ilustração a seguir mostrando a conetividade entre sistemas ONTAP e LUNs de array, as portas HBA 0a a 0d são usadas para conetividade com LUNs de storage porque as portas 1a a 1D são usadas para conetividade com discos:



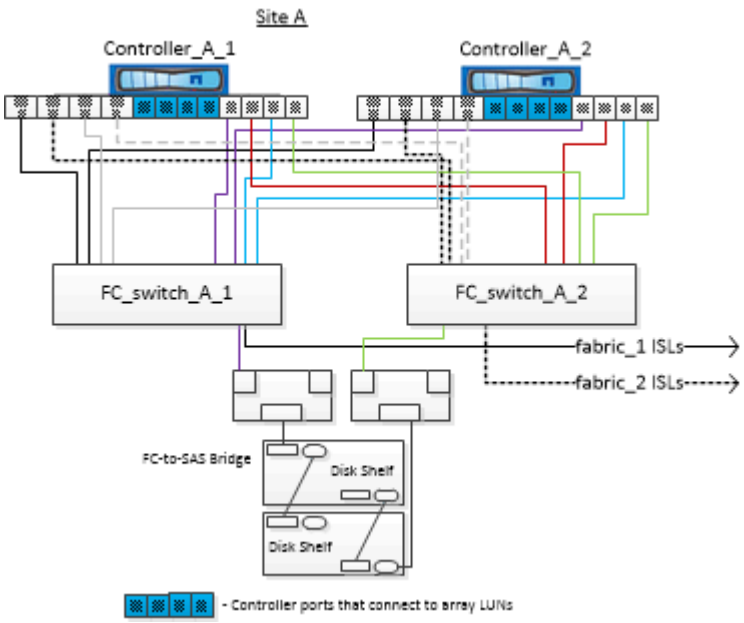
Exemplo de uma configuração de MetroCluster de quatro nós com discos e LUNs de array

Para configurar uma configuração de MetroCluster de quatro nós com discos nativos e LUNs de array, é necessário usar pontes FC para SAS para conectar os sistemas ONTAP aos compartimentos de disco por meio dos switches FC. É possível conectar LUNs de array por meio dos switches FC aos sistemas ONTAP.

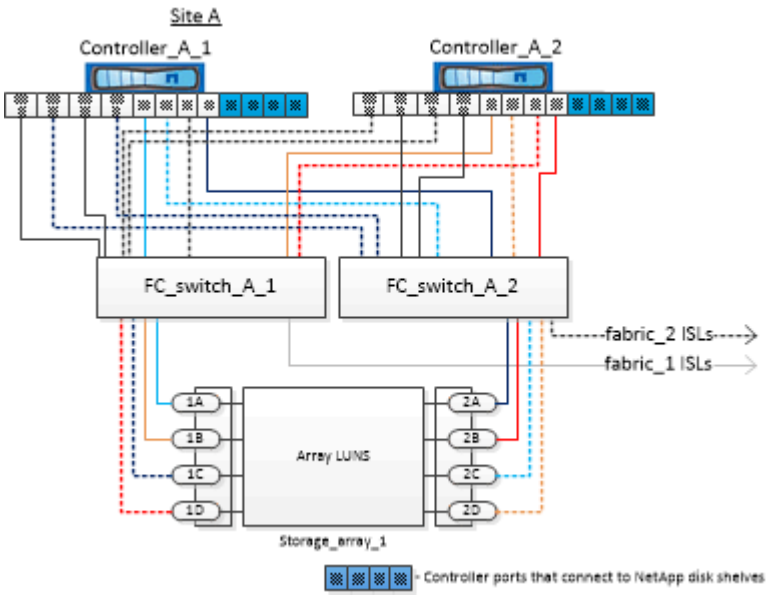
É necessário um mínimo de oito portas de iniciador para que um sistema ONTAP se conete a discos nativos e LUNs de storage.

As ilustrações a seguir representam exemplos de uma configuração MetroCluster com discos e LUNs de array. Ambas representam a mesma configuração MetroCluster; as representações para discos e LUNs de array são separadas apenas para simplificação.

Na ilustração a seguir, que mostra a conectividade entre sistemas ONTAP e discos, as portas HBA 1a a 1D são usadas para conetividade com discos por meio das pontes FC-para-SAS:



Na ilustração a seguir, que mostra a conetividade entre sistemas ONTAP e LUNs de storage, as portas HBA 0a a 0d são usadas para conetividade com LUNs de storage porque as portas 1a a 1D são usadas para conetividade com discos:



Como usar o Active IQ Unified Manager e o Gerenciador de sistemas ONTAP para configuração e monitoramento adicionais

Sincronizar a hora do sistema usando NTP

Cada cluster precisa de seu próprio servidor NTP (Network Time Protocol) para sincronizar o tempo entre os nós e seus clientes. Você pode usar a caixa de diálogo Editar DateTime no System Manager para configurar o servidor NTP.

Antes de começar

Você deve ter baixado e instalado o System Manager. O Gerenciador do sistema está disponível no site de suporte da NetApp.

Sobre esta tarefa

- Você não pode modificar as configurações de fuso horário para um nó com falha ou para o nó do parceiro após uma tomada de controle ocorrer.
- Cada cluster na configuração MetroCluster FC deve ter seu próprio servidor NTP separado ou servidores usados pelos nós, switches FC e pontes FC para SAS nesse local do MetroCluster.

  Se você estiver usando o software tiebreaker do MetroCluster, ele também deve ter seu próprio servidor NTP separado.

Passos

1. Na página inicial, clique duas vezes no sistema de armazenamento apropriado.
2. Expanda a hierarquia **Cluster** no painel de navegação esquerdo.
3. No painel de navegação, clique em **Configuração** > **Ferramentas do sistema** > **DateTime**.

4. Clique em **Editar**.
5. Selecione o fuso horário.
6. Especifique os endereços IP dos servidores de hora e clique em **Adicionar**.

   Você deve adicionar um servidor NTP à lista de servidores de hora. O controlador de domínio pode ser um servidor autorizado.

7. Clique em **OK**.
8. Verifique as alterações feitas nas configurações de data e hora na janela **Data e hora**.

Considerações ao usar o ONTAP em uma configuração do MetroCluster

Ao usar o ONTAP em uma configuração do MetroCluster, você deve estar ciente de certas considerações sobre licenciamento, peering para clusters fora da configuração do MetroCluster, execução de operações de volume, operações NVFAIL e outras operações do ONTAP.

Considerações sobre licenciamento

- Ambos os sites devem ser licenciados para os mesmos recursos licenciados pelo site.
- Todos os nós devem ser licenciados para os mesmos recursos de bloqueio de nó.

Consideração de SnapMirror

- A recuperação de desastres do SnapMirror SVM só é compatível com configurações do MetroCluster executando versões do ONTAP 9.5 ou posterior.

Suporte FlexCache em uma configuração MetroCluster

A partir do ONTAP 9.7, os volumes FlexCache são compatíveis com configurações do MetroCluster. Você deve estar ciente dos requisitos para a repetibilidade manual após operações de comutação ou switchback.

Repetibilidade da SVM após o switchover quando a origem e o cache do FlexCache estão no mesmo local do MetroCluster

Após um switchover negociado ou não planejado, qualquer relacionamento de peering SVM FlexCache no cluster deve ser configurado manualmente.

Por exemplo, SVMs "VS1" (cache) e "VS2" (origem) estão no site_A. Esses SVMs são peered.

Após o switchover, os SVMs "VS1-mc" e "VS2-mc" são ativados no local do parceiro (site_B). Eles devem ser manualmente repelidos para que o FlexCache funcione usando o `vserver peer repeer` comando.

Repetibilidade da SVM após switchover ou switchback quando um destino FlexCache está em um terceiro cluster e no modo desconetado

Para relacionamentos do FlexCache com um cluster fora da configuração do MetroCluster, o peering deve ser sempre reconfigurado manualmente após um switchover, se os clusters envolvidos estiverem no modo desconetado durante o switchover.

Por exemplo:

- Um fim do FlexCache (cache_1 no VS1) está alojado no MetroCluster site_A.
- A outra extremidade do FlexCache (origin_1 no VS2) reside no site_C (não na configuração do MetroCluster).

Quando o switchover é acionado e se o site_A e o site_C não estiverem conetados, você deverá repelir manualmente os SVMs no site_B (o cluster de switchover) e site_C usando o `vserver peer repeer` comando após o switchover.

Quando o switchback é executado, você deve repelir novamente os SVMs no site_A (o cluster original) e site_C.

Informações relacionadas

"Gerenciamento de volumes do FlexCache com a CLI"

Suporte FabricPool em configurações MetroCluster

A partir do ONTAP 9.7, as configurações do MetroCluster são compatíveis com camadas de storage FabricPool.

Para obter informações gerais sobre como usar o FabricPools, "Gerenciamento de disco e camada (agregado)"consulte .

Considerações ao usar FabricPools

- Os clusters precisam ter licenças FabricPool com limites de capacidade correspondentes.
- Os clusters devem ter IPspaces com nomes correspondentes.

  Esse pode ser o IPspace padrão ou um IPspace criado por um administrador. Este espaço IPspace será usado para configurações de armazenamento de objetos FabricPool.

- Para o espaço IPspace selecionado, cada cluster deve ter um LIF entre clusters definido que possa alcançar o armazenamento de objetos externo

Configurando um agregado para uso em um FabricPool espelhado

Antes de configurar o agregado, você deve configurar armazenamentos de objetos conforme descrito em "Configurar armazenamentos de objetos para FabricPool em uma configuração MetroCluster".

Passos

Para configurar um agregado para uso em um FabricPool:

1. Crie o agregado ou selecione um agregado existente.
2. Espelhe o agregado como um agregado espelhado típico na configuração do MetroCluster.
3. Crie o espelho FabricPool com o agregado, conforme descrito em "Gerenciamento de discos e agregados"
   a. Anexe um armazenamento de objetos primário.

      Este armazenamento de objetos está fisicamente mais perto do cluster.

   b. Adicione um armazenamento de objetos espelhados.

Este armazenamento de objetos está fisicamente mais distante do cluster do que o armazenamento de objetos primário.

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

Suporte FlexGroup em configurações MetroCluster

A partir do ONTAP 9.6, as configurações do MetroCluster são compatíveis com volumes FlexGroup.

Suporte a grupos de consistência nas configurações do MetroCluster

A partir do ONTAP 9.11,1, "grupos de consistência" são suportados nas configurações do MetroCluster.

Programações de trabalhos em uma configuração MetroCluster

No ONTAP 9.3 e posterior, as programações de tarefas criadas pelo usuário são replicadas automaticamente entre clusters em uma configuração do MetroCluster. Se você criar, modificar ou excluir um agendamento de trabalho em um cluster, o mesmo agendamento será criado automaticamente no cluster de parceiros, usando o CRS (Configuration Replication Service).

> As programações criadas pelo sistema não são replicadas e você deve executar manualmente a mesma operação no cluster de parceiros para que as programações de tarefas em ambos os clusters sejam idênticas.

Peering de cluster do site MetroCluster para um terceiro cluster

Como a configuração de peering não é replicada, se você identificar um dos clusters na configuração do MetroCluster para um terceiro cluster fora dessa configuração, você também deverá configurar o peering no cluster do MetroCluster parceiro. Isso é para que o peering possa ser mantido se ocorrer um switchover.

O cluster que não é MetroCluster deve estar executando o ONTAP 8,3 ou posterior. Caso contrário, o peering é perdido se ocorrer um switchover, mesmo que o peering tenha sido configurado em ambos os parceiros da MetroCluster.

Replicação de configuração de cliente LDAP em uma configuração MetroCluster

Uma configuração de cliente LDAP criada em uma máquina virtual de storage (SVM) em um cluster local é replicada para os dados de parceiros SVM no cluster remoto. Por exemplo, se a configuração do cliente LDAP for criada no SVM admin no cluster local, ela será replicada para todos os SVMs de dados administrativos no cluster remoto. Esse recurso do MetroCluster é intencional para que a configuração do cliente LDAP esteja ativa em todos os SVMs de parceiros no cluster remoto.

Diretrizes de criação de LIF e rede para configurações do MetroCluster

Você deve estar ciente de como LIFs são criados e replicados em uma configuração do MetroCluster. Você também deve saber sobre o requisito de consistência para que você possa tomar as decisões adequadas ao

configurar sua rede.

Informações relacionadas

- "Gerenciamento de rede e LIF"
- Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

  Requisitos de replicação de objeto IPspace e configuração de sub-rede

- Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

  Requisitos para criação de LIF em uma configuração MetroCluster

- Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

  Requisitos e problemas de replicação e posicionamento de LIF

Requisitos de replicação de objeto IPspace e configuração de sub-rede

Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

Replicação IPspace

Você deve considerar as diretrizes a seguir enquanto replica objetos IPspace para o cluster de parceiros:

- Os nomes de IPspace dos dois locais devem corresponder.
- Os objetos IPspace devem ser replicados manualmente para o cluster do parceiro.

  Quaisquer máquinas virtuais de armazenamento (SVMs) que sejam criadas e atribuídas a um IPspace antes que o IPspace seja replicado não serão replicadas para o cluster de parceiros.

Configuração de sub-rede

Você deve considerar as seguintes diretrizes ao configurar sub-redes em uma configuração do MetroCluster:

- Ambos os clusters da configuração do MetroCluster devem ter uma sub-rede no mesmo espaço IPspace com o mesmo nome de sub-rede, sub-rede, domínio de broadcast e gateway.
- Os intervalos de IP dos dois clusters devem ser diferentes.

  No exemplo a seguir, os intervalos de IP são diferentes:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------       -------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      --------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.21-192.168.2.30
```

Configuração IPv6

Se o IPv6 estiver configurado em um site, o IPv6 também deve ser configurado no outro site.

Informações relacionadas

- Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

  Requisitos para criação de LIF em uma configuração MetroCluster

- Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

  Requisitos e problemas de replicação e posicionamento de LIF

Requisitos para criação de LIF em uma configuração MetroCluster

Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

Você deve considerar as seguintes diretrizes ao criar LIFs:

- Fibre Channel: Você precisa usar VSAN esticada ou tecidos esticados
- IP/iSCSI: Você deve usar a rede estendida da camada 2
- Broadcasts ARP: Você deve habilitar broadcasts ARP entre os dois clusters
- LIFs duplicadas: Você não deve criar vários LIFs com o mesmo endereço IP (LIFs duplicadas) em um espaço IPspace

- Configurações NFS e SAN: Você precisa usar diferentes máquinas virtuais de storage (SVMs) para agregados sem espelhamento e espelhados
- Você deve criar um objeto de sub-rede antes de criar um LIF. Um objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque tem um domínio de broadcast associado.

Verifique a criação de LIF

Você pode confirmar a criação bem-sucedida de um LIF em uma configuração do MetroCluster executando o `metrocluster check lif show` comando. Se você encontrar algum problema ao criar o LIF, você pode usar o `metrocluster check lif repair-placement` comando para corrigir os problemas.

Informações relacionadas

- Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

  Requisitos de replicação de objeto IPspace e configuração de sub-rede

- Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

  Requisitos e problemas de replicação e posicionamento de LIF

Requisitos e problemas de replicação e posicionamento de LIF

Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

Replicação de LIFs para o cluster de parceiros

Quando você cria um LIF em um cluster em uma configuração do MetroCluster, o LIF é replicado no cluster de parceiros. LIFs não são colocados em uma base de nome individual. Para disponibilidade de LIFs após uma operação de switchover, o processo de colocação de LIF verifica se as portas são capazes de hospedar o LIF com base em verificações de acessibilidade e atributos de porta.

O sistema deve atender às seguintes condições para colocar as LIFs replicadas no cluster de parceiros:

Condição	Tipo de LIF: FC	Tipo de LIF: IP/iSCSI
Identificação do nó	O ONTAP tenta colocar o LIF replicado no parceiro de recuperação de desastres (DR) do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.	O ONTAP tenta colocar o LIF replicado no parceiro de DR do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.

Identificação da porta	O ONTAP identifica as portas de destino FC conectadas no cluster de DR.	As portas no cluster de DR que estão no mesmo espaço IPspace que o LIF de origem são selecionadas para uma verificação de acessibilidade. Se não houver portas no cluster de DR no mesmo IPspace, o LIF não pode ser colocado. Todas as portas no cluster de DR que já estão hospedando um LIF no mesmo espaço IPspace e sub-rede são marcadas automaticamente como alcançáveis e podem ser usadas para o posicionamento. Essas portas não estão incluídas na verificação de acessibilidade.
Verificação de acessibilidade	A acessibilidade é determinada verificando a conetividade da malha de origem WWN nas portas do cluster de DR. Se a mesma malha não estiver presente no local de DR, o LIF será colocado em uma porta aleatória no parceiro de DR.	A acessibilidade é determinada pela resposta a um broadcast ARP (Address Resolution Protocol) de cada porta identificada anteriormente no cluster de DR para o endereço IP de origem do LIF a ser colocado. Para que as verificações de acessibilidade sejam bem-sucedidas, os broadcasts ARP devem ser permitidos entre os dois clusters. Cada porta que recebe uma resposta do LIF de origem será marcada como possível para o posicionamento.

Seleção da porta	O ONTAP categoriza as portas com base em atributos como tipo e velocidade do adaptador e, em seguida, seleciona as portas com atributos correspondentes. Se nenhuma porta com atributos correspondentes for encontrada, o LIF será colocado em uma porta conetada aleatória no parceiro DR.	A partir das portas marcadas como alcançáveis durante a verificação de acessibilidade, o ONTAP prefere as portas que estão no domínio de broadcast associado à sub-rede do LIF. Se não houver portas de rede disponíveis no cluster de DR que estejam no domínio de broadcast associado à sub-rede do LIF, o ONTAP selecionará portas que tenham acessibilidade ao LIF de origem. Se não houver portas com acessibilidade ao LIF de origem, uma porta será selecionada do domínio de broadcast associado à sub-rede do LIF de origem e, se nenhum domínio de broadcast existir, uma porta aleatória será selecionada. O ONTAP categoriza as portas com base em atributos como tipo de adaptador, tipo de interface e velocidade e, em seguida, seleciona as portas com atributos correspondentes.
Colocação de LIF	A partir das portas alcançáveis, o ONTAP seleciona a porta menos carregada para colocação.	A partir das portas selecionadas, o ONTAP seleciona a porta menos carregada para colocação.

Colocação de LIFs replicadas quando o nó do parceiro de DR está inativo

Quando um iSCSI ou FC LIF é criado em um nó cujo parceiro de DR foi assumido, o LIF replicado é colocado no nó do parceiro auxiliar de DR. Após uma operação subsequente de giveback, os LIFs não são movidos automaticamente para o parceiro DR. Isso pode levar a que os LIFs se concentrem em um único nó no cluster de parceiros. Durante uma operação de switchover do MetroCluster, tentativas subsequentes de mapear LUNs pertencentes à máquina virtual de storage (SVM) falham.

Você deve executar o `metrocluster check lif show` comando após uma operação de aquisição ou operação de giveback para verificar se o posicionamento de LIF está correto. Se existirem erros, pode executar o `metrocluster check lif repair-placement` comando para resolver os problemas.

Erros de colocação de LIF

Os erros de colocação de LIF que são exibidos pelo `metrocluster check lif show` comando são retidos após uma operação de comutação. Se o `network interface modify` comando , `network interface rename` ou `network interface delete` for emitido para um LIF com um erro de posicionamento, o erro será removido e não aparecerá na saída do `metrocluster check lif show` comando.

Falha de replicação de LIF

Você também pode verificar se a replicação do LIF foi bem-sucedida usando o `metrocluster check lif show` comando. Uma mensagem EMS é exibida se a replicação LIF falhar.

Você pode corrigir uma falha de replicação executando o `metrocluster check lif repair-placement` comando para qualquer LIF que não consiga encontrar uma porta correta. Você deve resolver quaisquer falhas de replicação de LIF o mais rápido possível para verificar a disponibilidade de LIF durante uma operação de switchover de MetroCluster.

> Mesmo que o SVM de origem esteja inativo, o posicionamento de LIF pode continuar normalmente se houver um LIF pertencente a um SVM diferente em uma porta com o mesmo espaço IPspace e rede no SVM de destino.

LIFs inacessíveis após uma mudança

Se for feita alguma alteração na malha de switch FC à qual as portas de destino FC dos nós de origem e DR estão conectadas, as LIFs FC colocadas no parceiro de DR podem ficar inacessíveis aos hosts após uma operação de switchover.

Você deve executar o `metrocluster check lif repair-placement` comando na origem e nos nós de DR após uma alteração na malha do switch FC para verificar a conectividade de host dos LIFs. As alterações na malha do switch podem resultar na colocação de LIFs em diferentes portas FC de destino no nó do parceiro de DR.

Informações relacionadas

- Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

  Requisitos de replicação de objeto IPspace e configuração de sub-rede

- Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

  Requisitos para criação de LIF em uma configuração MetroCluster

Criação de volume em um agregado raiz

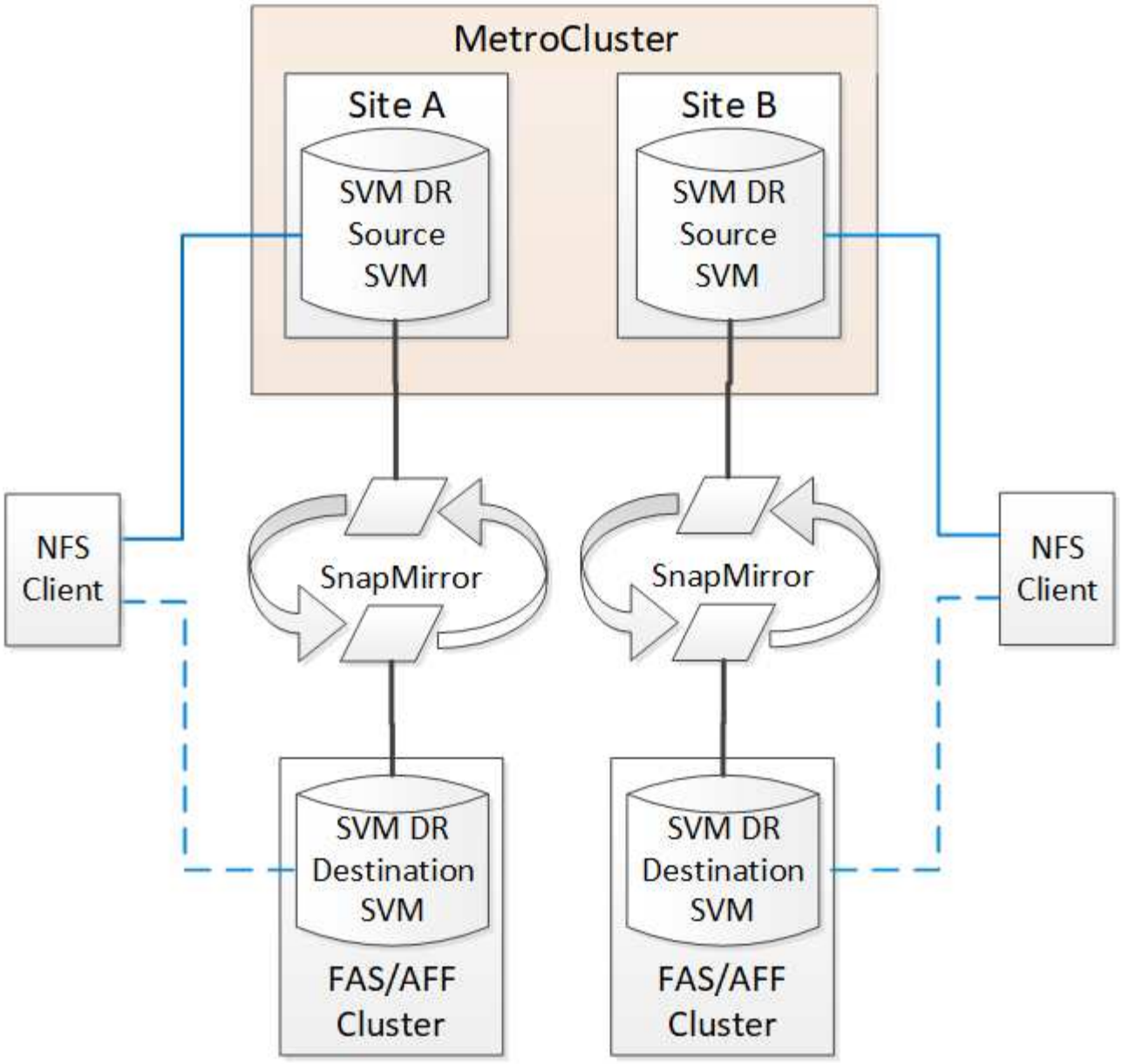
O sistema não permite a criação de novos volumes no agregado raiz (um agregado com uma política de HA do CFO) de um nó em uma configuração do MetroCluster.

Devido a essa restrição, os agregados de raiz não podem ser adicionados a um SVM usando o `vserver add-aggregates` comando.

Recuperação de desastres do SVM em uma configuração de MetroCluster

A partir do ONTAP 9.5, as máquinas virtuais de storage ativo (SVMs) em uma configuração do MetroCluster podem ser usadas como fontes com o recurso de recuperação de desastres do SnapMirror SVM. O SVM de destino deve estar no terceiro cluster fora da configuração do MetroCluster.

A partir do ONTAP 9.11,1, ambos os locais em uma configuração do MetroCluster podem ser a origem de uma relação de SVM DR com um cluster de destino FAS ou AFF, conforme mostrado na imagem a seguir.



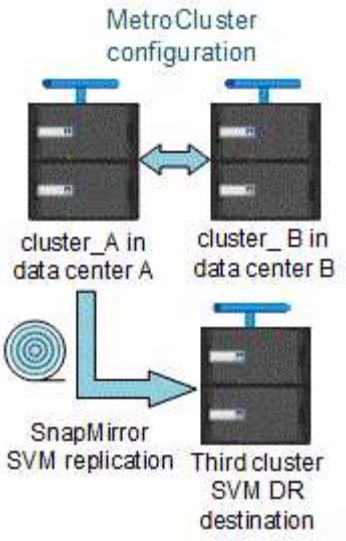
Você deve estar ciente dos seguintes requisitos e limitações de uso de SVMs com recuperação de desastres do SnapMirror:

- Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM.

  Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover.

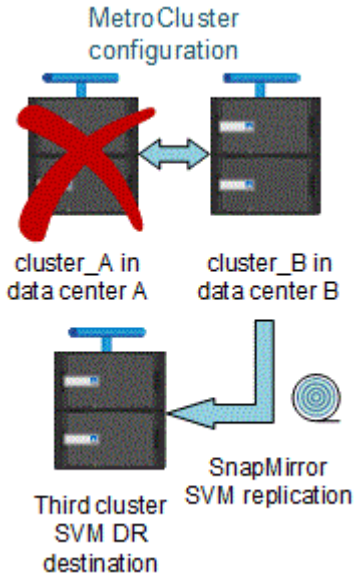
- Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online.

  A imagem a seguir mostra o comportamento de recuperação de desastres do SVM em um estado estável:



- Quando o SVM de origem sincronizada é a fonte de uma relação SVM DR, as informações de origem no relacionamento de SVM DR são replicadas para o parceiro MetroCluster.

  Isso permite que as atualizações do SVM DR continuem após um switchover, conforme mostrado na imagem a seguir:



- Durante os processos de switchover e switchback, a replicação para o destino SVM DR pode falhar.

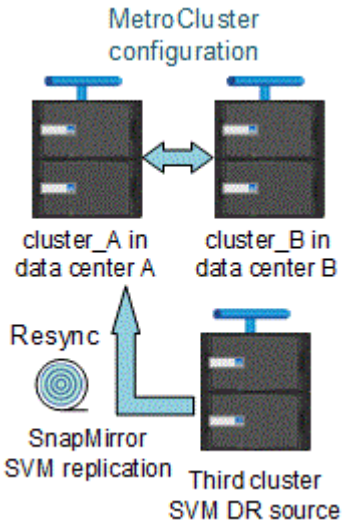
  No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas do SVM DR serão bem-sucedidas.

Consulte a seção ""replicando a configuração do SVM"" no "Proteção de dados com a CLI" para obter detalhes sobre como configurar um relacionamento de DR do SVM.

Ressincronização da SVM em um local de recuperação de desastre

Durante a ressincronização, a fonte de recuperação de desastres (DR) de máquinas virtuais de storage (SVMs) na configuração MetroCluster é restaurada a partir do SVM de destino no local que não é MetroCluster.

Durante a ressincronização, o SVM de origem (cluster_A) atua temporariamente como SVM de destino, conforme mostrado na imagem a seguir:



Se um switchover não planejado ocorrer durante a ressincronização

Switchovers não planejados que ocorrem durante a ressincronização interromperão a transferência de ressincronização. Se ocorrer um switchover não planejado, as seguintes condições são verdadeiras:

- O SVM de destino no local do MetroCluster (que era uma fonte SVM antes da ressincronização) permanece como um SVM de destino. O SVM no cluster de parceiros continuará mantendo seu subtipo e inativo.
- A relação do SnapMirror deve ser recriada manualmente com o SVM de destino de sincronização como destino.
- A relação SnapMirror não aparece na saída do show do SnapMirror após um switchover no local sobrevivente, a menos que uma operação de criação do SnapMirror seja executada.

Execução do switchback após um switchover não planejado durante a ressincronização

Para executar com sucesso o processo de switchback, a relação de ressincronização deve ser quebrada e excluída. O switchback não é permitido se houver algum SVMs de destino de DR do SnapMirror na configuração do MetroCluster ou se o cluster tiver um SVM de subtipo "dp-destination".

A saída para o comando "storage Aggregate plex show" é indeterminada após um switchover do MetroCluster

Quando você executa o `storage aggregate plex show` comando após um switchover MetroCluster, o status de plex0 do agregado raiz comutada é indeterminado e é exibido como "failed". Durante este tempo, a raiz comutada não é atualizada. O estado real deste Plex só pode ser determinado após a fase de cicatrização do MetroCluster.

Modificação de volumes para definir o sinalizador NVFAIL em caso de comutação

Você pode modificar um volume para que o sinalizador NVFAIL seja definido no volume em caso de um switchover MetroCluster. O sinalizador NVFAIL faz com que o volume seja vedado de qualquer modificação. Isso é necessário para volumes que precisam ser tratados como se as gravações confirmadas no volume fossem perdidas após o switchover.

Sobre esta tarefa

Nas versões do ONTAP anteriores a 9,0, o sinalizador NVFAIL é usado para cada switchover. No ONTAP 9.0 e versões posteriores, o switchover não planejado (USO) é usado.

Passo

1. Ative a configuração do MetroCluster para acionar o NVFAIL no switchover definindo o `vol -dr-force -nvfail` parâmetro para "On":

   `vol modify -vserver` *`vserver-name`* `-volume` *`volume-name`* `-dr-force-nvfail on`

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Documentação do ONTAP 9"	• Todas as informações do MetroCluster
"Arquitetura e Design de soluções da NetApp MetroCluster, TR-4705"	• Uma visão geral técnica da configuração e operação do MetroCluster FC. • Práticas recomendadas para configuração MetroCluster FC.
"Arquitetura e design da solução IP da MetroCluster, TR-4689"	• Uma visão geral técnica da configuração e operação do MetroCluster IP. • Práticas recomendadas para a configuração IP do MetroCluster.
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Instalação e configuração do IP MetroCluster: Diferenças entre as configurações do ONTAP MetroCluster"	• Arquitetura IP do MetroCluster • Fazer o cabeamento da configuração • Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster e recuperação de desastres"	• Compreender a configuração do MetroCluster • Switchover, cura e switchback • Recuperação de desastres

"Mantenha os componentes do MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster FC • Procedimentos de substituição ou atualização de hardware e atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conetada à malha • Substituição de hardware em um local de desastre em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.
"Transição do MetroCluster FC para o MetroCluster IP" "Guia de atualização e expansão do MetroCluster"	• Atualizando ou atualizando uma configuração do MetroCluster • Transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP • Expansão de uma configuração do MetroCluster com a adição de nós adicionais
"Instalação e configuração do software MetroCluster Tiebreaker"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
Documentação do consultor digital da Active IQ "Documentação do NetApp: Guias de produto e recursos"	• Monitoramento da configuração e do desempenho do MetroCluster
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
"Conceitos de ONTAP"	• Como os agregados espelhados funcionam

Instale uma configuração IP do MetroCluster

Visão geral

Para instalar sua configuração IP do MetroCluster, você deve executar vários procedimentos na ordem correta.

- "Prepare-se para a instalação e entenda todos os requisitos".
- "Faça o cabo dos componentes"
- "Configure o software"
- "Configurar o ONTAP Mediator" (opcional)
- "Teste a configuração"

Prepare-se para a instalação do MetroCluster

Diferenças entre as configurações do ONTAP MetroCluster

As várias configurações do MetroCluster têm diferenças importantes nos componentes necessários.

Em todas as configurações, cada um dos dois locais do MetroCluster é configurado como um cluster do ONTAP. Em uma configuração de MetroCluster de dois nós, cada nó é configurado como um cluster de nó único.

Recurso	Configurações IP	Configurações conectadas à malha		Configurações elásticas	
		Quatro ou oito nós	* Dois nós*	* Dois nós bridge-attached*	**Conexão direta de dois nós**
Número de controladores	Quatro ou oito*	Quatro ou oito	Dois	Dois	Dois
Usa uma malha de storage de switch FC	Não	Sim	Sim	Não	Não
Usa uma malha de storage de switch IP	Sim	Não	Não	Não	Não
Usa pontes FC para SAS	Não	Sim	Sim	Sim	Não
Usa o storage SAS com conexão direta	Sim (apenas anexo local)	Não	Não	Não	Sim

Suporta ADP	Sim (começando com ONTAP 9.4)	Não	Não	Não	Não
Suporta HA local	Sim	Sim	Não	Não	Não
Compatível com o switchover não planejado automático do ONTAP (AUSO)	Não	Sim	Sim	Sim	Sim
Compatível com agregados sem espelhamento	Sim (começando com ONTAP 9.8)	Sim	Sim	Sim	Sim
Compatível com LUNs de array	Não	Sim	Sim	Sim	Sim
Suporta o Mediador ONTAP	Sim (começando com ONTAP 9.7)	Não	Não	Não	Não
Compatível com o tiebreaker MetroCluster	Sim (não em combinação com o Mediador ONTAP)	Sim	Sim	Sim	Sim
Suportes Todos os arrays SAN	Sim	Sim	Sim	Sim	Sim

Importante

Observe as seguintes considerações para configurações de IP MetroCluster de oito nós:

- As configurações de oito nós são suportadas a partir do ONTAP 9.9,1.
- Somente switches MetroCluster validados pela NetApp (solicitados pela NetApp) são compatíveis.
- Configurações que usam conexões de back-end roteadas por IP (camada 3) não são suportadas.
- As configurações que usam redes de camada privada compartilhada 2 não são suportadas.
- As configurações que usam um switch compartilhado Cisco 9336C-FX2 não são suportadas.

Suporte para todos os sistemas de storage SAN nas configurações do MetroCluster

Alguns dos All SAN Arrays (ASAs) são suportados nas configurações do MetroCluster. Na documentação do MetroCluster, as informações dos modelos AFF aplicam-se ao sistema ASA correspondente. Por exemplo, todo o cabeamento e outras informações do sistema AFF A400 também se aplicam ao sistema ASA AFF A400.

As configurações de plataforma compatíveis estão listadas no "NetApp Hardware Universe".

Diferenças entre ONTAP Mediator e MetroCluster tiebreaker

A partir do ONTAP 9.7, você pode usar o switchover não planejado automático assistido por Mediador ONTAP (MAUSO) na configuração IP do MetroCluster ou você pode usar o software tiebreaker do MetroCluster. Não é necessário usar o software MAUSO ou tiebreaker; no entanto, se você optar por não usar nenhum desses serviços, será necessário "realize uma recuperação manual" se ocorrer um desastre.

As diferentes configurações do MetroCluster executam o switchover automático em diferentes circunstâncias:

- **Configurações MetroCluster FC usando a capacidade AUSO (não presente nas configurações IP do MetroCluster)**

  Nessas configurações, o AUSO é iniciado se os controladores falharem, mas o armazenamento (e as bridges, se presentes) permanecem operacionais.

- **Configurações IP do MetroCluster usando o serviço Mediador ONTAP (ONTAP 9.7 e posterior)**

  Nessas configurações, o MAUSO é iniciado nas mesmas circunstâncias que o AUSO, conforme descrito acima, e também após uma falha completa do local (controladores, armazenamento e switches).

  "Saiba mais sobre como o Mediador ONTAP suporta switchover não planejado automático".

- **Configurações MetroCluster IP ou FC usando o software tiebreaker no modo ativo**

  Nessas configurações, o tiebreaker inicia o switchover não planejado após uma falha completa no local.

  Antes de utilizar o software tiebreaker, reveja o. "Instalação e configuração do software MetroCluster Tiebreaker"

Interoperabilidade do ONTAP Mediator com outros aplicativos e dispositivos

Você não pode usar aplicativos ou dispositivos de terceiros que possam acionar um switchover em combinação com o ONTAP Mediator. Além disso, o monitoramento de uma configuração do MetroCluster com o software tiebreaker MetroCluster não é suportado ao usar o ONTAP Mediator.

Considerações para configurações IP do MetroCluster

Você deve entender como os controladores acessam o armazenamento remoto e como os endereços IP do MetroCluster funcionam.

Acesso ao armazenamento remoto em configurações IP do MetroCluster

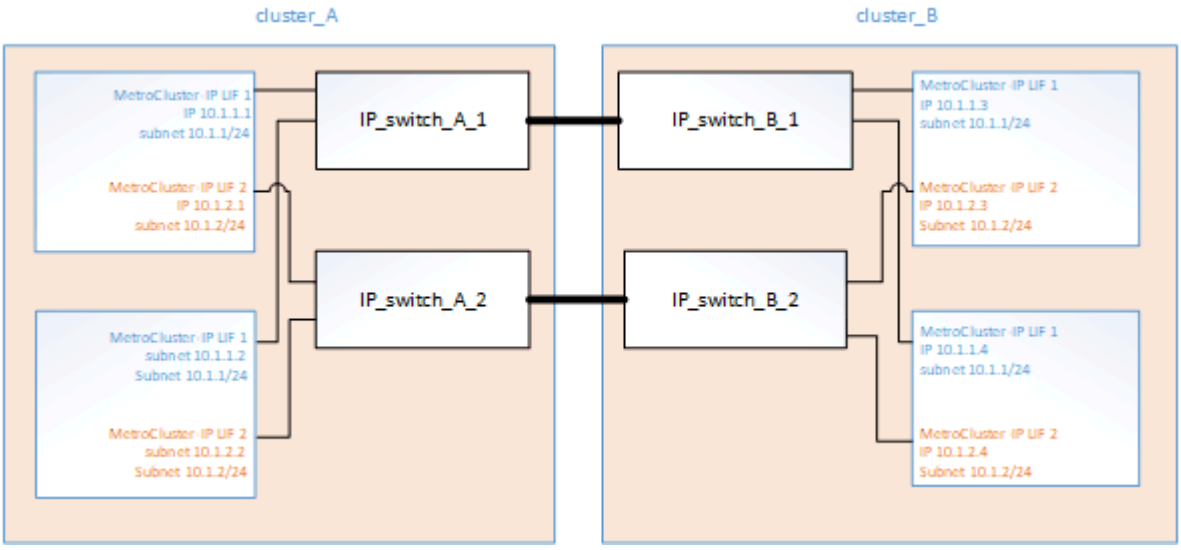
Nas configurações IP do MetroCluster, a única maneira de os controladores locais chegarem aos pools de armazenamento remoto é através dos controladores remotos. Os switches IP são conetados às portas Ethernet dos controladores; eles não têm conexões diretas com as gavetas de disco. Se o controle remoto estiver inativo, os controladores locais não poderão alcançar seus pools de armazenamento remoto.

Isso é diferente das configurações de FC MetroCluster, nas quais os pools de storage remoto são conectados às controladoras locais por meio da malha FC ou das conexões SAS. Os controladores locais ainda têm acesso ao armazenamento remoto, mesmo que os controladores remotos estejam inativos.

Endereços IP MetroCluster

Você deve estar ciente de como os endereços IP e interfaces do MetroCluster são implementados em uma configuração IP do MetroCluster, bem como os requisitos associados.

Em uma configuração IP do MetroCluster, a replicação do storage e do cache não volátil entre os pares de HA e os parceiros de DR é realizada por meio de links dedicados de alta largura de banda na malha IP do MetroCluster. As conexões iSCSI são usadas para replicação de storage. Os switches IP também são usados para todo o tráfego intra-cluster dentro dos clusters locais. O tráfego MetroCluster é mantido separado do tráfego intra-cluster usando sub-redes IP e VLANs separadas. A malha IP do MetroCluster é distinta e diferente da rede de peering de cluster.



A configuração IP do MetroCluster requer dois endereços IP em cada nó que são reservados para a malha IP do MetroCluster de back-end. Os endereços IP reservados são atribuídos a interfaces lógicas IP (LIFs) MetroCluster durante a configuração inicial e têm os seguintes requisitos:

> Você deve escolher os endereços IP do MetroCluster cuidadosamente, porque não pode alterá-los após a configuração inicial.

- Eles devem cair em um intervalo IP único.

  Eles não devem se sobrepor a qualquer espaço IP no ambiente.

- Eles devem residir em uma das duas sub-redes IP que as separam de todo o outro tráfego.

Por exemplo, os nós podem ser configurados com os seguintes endereços IP:

Nó	Interface	Endereço IP	Sub-rede
node_A_1	Interface IP MetroCluster 1	10.1.1.1	10,1.1/24
node_A_1	Interface IP MetroCluster 2	10.1.2.1	10,1.2/24

node_A_2	Interface IP MetroCluster 1	10.1.1.2	10,1.1/24
node_A_2	Interface IP MetroCluster 2	10.1.2.2	10,1.2/24
node_B_1	Interface IP MetroCluster 1	10.1.1.3	10,1.1/24
node_B_1	Interface IP MetroCluster 2	10.1.2.3	10,1.2/24
node_B_2	Interface IP MetroCluster 1	10.1.1.4	10,1.1/24
node_B_2	Interface IP MetroCluster 2	10.1.2.4	10,1.2/24

Caraterísticas das interfaces IP MetroCluster

As interfaces IP do MetroCluster são específicas para configurações IP do MetroCluster. Eles têm caraterísticas diferentes de outros tipos de interface ONTAP:

- Eles são criados pelo `metrocluster configuration-settings interface create` comando como parte da configuração inicial do MetroCluster.

  A partir do ONTAP 9.9,1, se você estiver usando uma configuração da camada 3, você também deve especificar o `-gateway` parâmetro ao criar interfaces IP do MetroCluster. "Considerações para redes de grande área da camada 3"Consulte a .

  Eles não são criados ou modificados pelos comandos da interface de rede.

- Eles não aparecem na saída do `network interface show` comando.
- Eles não falham, mas permanecem associados com a porta em que foram criados.
- As configurações IP do MetroCluster usam portas Ethernet específicas (dependendo da plataforma) para as interfaces IP do MetroCluster.

Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior

A partir do ONTAP 9.4, as configurações IP do MetroCluster suportam novas instalações usando atribuição automática de disco e ADP (particionamento avançado de unidade).

Você deve estar ciente das seguintes considerações ao usar ADP com configurações IP do MetroCluster:

- O ONTAP 9.4 e posterior são necessários para usar o ADP com configurações MetroCluster IP em sistemas AFF e ASA.
- O ADPv2 é compatível com configurações IP do MetroCluster.

- O agregado raiz deve estar localizado na partição 3 para todos os nós em ambos os locais.
- O particionamento e a atribuição de disco são executados automaticamente durante a configuração inicial dos sites do MetroCluster.
- As atribuições de disco do pool 0 são feitas na fábrica.
- A raiz sem espelhamento é criada na fábrica.
- A atribuição de partição de dados é feita no local do cliente durante o procedimento de configuração.
- Na maioria dos casos, a atribuição e o particionamento de unidades são feitos automaticamente durante os procedimentos de configuração.
- Um disco e todas as partições precisam ser de propriedade de nós no mesmo par de alta disponibilidade (HA). A propriedade de partição ou unidade em uma única unidade não pode ser misturada entre o par de HA local e o parceiro de recuperação de desastres (DR) ou parceiro auxiliar de DR.

  Exemplo de uma configuração suportada:

Unidade/partição	Proprietário
Unidade:	`ClusterA-Node01`
Partição 1:	`ClusterA-Node01`
Partição 2:	`ClusterA-Node02`
Partição 3:	`ClusterA-Node01`

Ao atualizar do ONTAP 9.4 para o 9,5, o sistema reconhece as atribuições de disco existentes.

Particionamento automático

O ADP é executado automaticamente durante a configuração inicial do sistema.

A partir do ONTAP 9.5, a atribuição automática de discos deve ser ativada com o `storage disk option modify -autoassign on` comando.

Você deve definir o estado ha-config como `mccip` antes do provisionamento automático para garantir que os tamanhos de partição corretos estejam selecionados para permitir o tamanho de volume raiz apropriado. Para obter mais informações, "Verificando o estado ha-config dos componentes"consulte .

Um máximo de 96 unidades pode ser particionado automaticamente durante a instalação. Você pode adicionar unidades extras após a instalação inicial.

Se você estiver usando unidades internas e externas, primeiro inicialize o MetroCluster apenas com as unidades internas usando ADP. Em seguida, conete manualmente o compartimento externo após concluir a tarefa de instalação ou configuração.

Você deve garantir que os compartimentos internos tenham o número mínimo recomendado de unidades, conforme descrito Diferenças de atribuição de ADP e disco por sistemaem .

Para as unidades internas e externas, é necessário preencher os compartimentos parcialmente completos, conforme descrito em Como preencher compartimentos parcialmente cheios.

Como funciona a atribuição automática prateleira a prateleira

Se houver quatro compartimentos externos por local, cada compartimento será atribuído a um nó diferente e um pool diferente, como mostrado no exemplo a seguir:

- Todos os discos no site_A-shelf_1 são atribuídos automaticamente ao pool 0 do node_A_1
- Todos os discos no site_A-shelf_3 são atribuídos automaticamente ao pool 0 do node_A_2
- Todos os discos no site_B-shelf_1 são atribuídos automaticamente ao pool 0 do node_B_1
- Todos os discos no site_B-shelf_3 são atribuídos automaticamente ao pool 0 do node_B_2
- Todos os discos no site_B-shelf_2 são atribuídos automaticamente ao pool 1 do node_A_1
- Todos os discos no site_B-shelf_4 são atribuídos automaticamente ao pool 1 do node_A_2
- Todos os discos no site_A-shelf_2 são atribuídos automaticamente ao pool 1 do node_B_1
- Todos os discos no site_A-shelf_4 são atribuídos automaticamente ao pool 1 do node_B_2

Como preencher compartimentos parcialmente cheios

Se a configuração estiver usando compartimentos que não estejam totalmente preenchidos (com compartimentos de unidade vazios), você deverá distribuir as unidades uniformemente por todo o compartimento, dependendo da política de atribuição de disco. A política de atribuição de disco depende de quantas gavetas estão em cada local do MetroCluster.

Se você estiver usando uma única gaveta em cada local (ou apenas a gaveta interna em um sistema AFF A800), os discos serão atribuídos usando uma política de quarto de compartimento. Se o compartimento não estiver totalmente preenchido, instale as unidades igualmente em todos os trimestres.

A tabela a seguir mostra um exemplo de como colocar 24 discos em um compartimento interno de 48 unidades. A propriedade das unidades também é mostrada.

Os 48 compartimentos de unidades estão divididos em quatro quartos:	Instale seis unidades nos primeiros seis compartimentos em cada trimestre…
Trimestre de 1: Baías 0-11	Baías 0-5
Trimestre de 2: Baías 12-23	Baías 12-17
Trimestre de 3: Baías 24-35	Baías 24-29
Trimestre de 4: Baías 36-47	Baías 36-41

A tabela a seguir mostra um exemplo de como colocar 16 discos em um compartimento interno de 24 unidades.

Os 24 compartimentos de unidades estão divididos em quatro quartos:	Instale quatro unidades nos primeiros quatro compartimentos em cada trimestre…
Trimestre de 1: Baías 0-5	Baías 0-3
Trimestre de 2: Baías 6-11	Baías 6-9

Trimestre de 3: Baías 12-17	Baías 12-15
Trimestre de 4: Baías 18-23	Baías 18-21

Se você estiver usando duas gavetas externas em cada local, os discos serão atribuídos usando uma política de meia gaveta. Se as gavetas não estiverem totalmente preenchidas, instale as unidades igualmente de uma das extremidades da gaveta.

Por exemplo, se você estiver instalando unidades de 12 TB em um compartimento de 24 unidades, instale as unidades nos compartimentos 0-5 e 18-23.

Atribuição manual de acionamento (ONTAP 9.5)

No ONTAP 9.5, a atribuição manual de unidades é necessária em sistemas com as seguintes configurações de gaveta:

- Três gavetas externas por local.

  Duas gavetas são atribuídas automaticamente usando uma política de atribuição de meia prateleira, mas o terceiro compartimento deve ser atribuído manualmente.

- Mais de quatro gavetas por local e o número total de gavetas externas não são várias de quatro.

  Gavetas extras acima do múltiplo mais próximo de quatro são deixadas sem atribuição e as unidades devem ser atribuídas manualmente. Por exemplo, se houver cinco compartimentos externos no local, o compartimento cinco deve ser atribuído manualmente.

Você só precisa atribuir manualmente uma única unidade em cada gaveta não atribuída. As outras unidades na gaveta são atribuídas automaticamente.

Atribuição manual de acionamento (ONTAP 9.4)

No ONTAP 9.4, a atribuição manual de unidades é necessária em sistemas com as seguintes configurações de gaveta:

- Menos de quatro gavetas externas por local.

  As unidades devem ser atribuídas manualmente para garantir a atribuição simétrica das unidades, com cada pool tendo um número igual de unidades.

- Mais de quatro gavetas externas por local e o número total de gavetas externas não são várias de quatro.

  Gavetas extras acima do múltiplo mais próximo de quatro são deixadas sem atribuição e as unidades devem ser atribuídas manualmente.

Ao atribuir manualmente unidades, você deve atribuir discos simetricamente, com um número igual de unidades atribuídas a cada pool. Por exemplo, se a configuração tiver dois compartimentos de storage em cada local, você faria uma gaveta para o par de HA local e uma gaveta para o par de HA remoto:

- Atribua metade dos discos no site_A-shelf_1 ao pool 0 do node_A_1.
- Atribua metade dos discos no site_A-shelf_1 ao pool 0 do node_A_2.

- Atribua metade dos discos no site_A-shelf_2 ao pool 1 do node_B_1.
- Atribua metade dos discos no site_A-shelf_2 ao pool 1 do node_B_2.
- Atribua metade dos discos no site_B-shelf_1 ao pool 0 do node_B_1.
- Atribua metade dos discos no site_B-shelf_1 ao pool 0 do node_B_2.
- Atribua metade dos discos no site_B-shelf_2 ao pool 1 do node_A_1.
- Atribua metade dos discos no site_B-shelf_2 ao pool 1 do node_A_2.

Adição de compartimentos a uma configuração existente

A atribuição automática de unidades dá suporte à adição simétrica de gavetas a uma configuração existente.

Quando novas gavetas são adicionadas, o sistema aplica a mesma política de atribuição a gavetas recém-adicionadas. Por exemplo, com uma única gaveta por local, se um compartimento adicional for adicionado, os sistemas aplicarão as regras de atribuição de um quarto de compartimento à nova gaveta.

Informações relacionadas

"Componentes IP do MetroCluster necessários e convenções de nomenclatura"

"Gerenciamento de disco e agregado"

Diferenças de atribuição de ADP e disco por sistema em configurações IP do MetroCluster

A operação de Advanced Drive Partitioning (ADP) e atribuição automática de disco nas configurações MetroCluster IP varia dependendo do modelo do sistema.

Em sistemas que usam ADP, agregados são criados usando partições nas quais cada unidade é particionada em partições P1, P2 e P3. O agregado raiz é criado usando partições P3.

Você deve atender aos limites do MetroCluster para o número máximo de unidades compatíveis e outras diretrizes.

"NetApp Hardware Universe"

ADP e atribuição de disco em sistemas AFF A320

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz

Mínimo de unidades recomendadas (por local)	48 unidades	As unidades em cada compartimento externo são divididas em dois grupos iguais (metades). Cada meia prateleira é atribuída automaticamente a um pool separado.	Uma gaveta é usada pelo par de HA local. O segundo compartimento é usado pelo par de HA remoto. **Partições em cada prateleira são usadas para criar o agregado raiz. Cada um dos dois plexes no agregado raiz inclui as seguintes partições** • Oito partições para dados • Duas partições de paridade • Duas partições de reposição
Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais. Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexes no agregado raiz inclui as seguintes partições: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

ADP e atribuição de disco em sistemas AFF A150, ASA A150 e AFF A220

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz

Mínimo de unidades recomendadas (por local)	Apenas unidades internas	As unidades internas são divididas em quatro grupos iguais. Cada grupo é atribuído automaticamente a um pool separado e cada pool é atribuído a um controlador separado na configuração. Metade das unidades internas permanecem sem atribuição antes de o MetroCluster ser configurado.	Dois trimestres são usados pelo par de HA local. Os outros dois trimestres são usados pelo par de HA remoto. O agregado raiz inclui as seguintes partições em cada Plex: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

Mínimo de unidades compatíveis (por local)	16 unidades internas	As unidades são divididas em quatro grupos iguais. Cada compartimento é atribuído automaticamente a um pool separado. Dois quartos em uma prateleira podem ter o mesmo pool. O pool é escolhido com base no nó proprietário do trimestre: • Se for propriedade do nó local, pool0 é usado. • Se for propriedade do nó remoto, pool1 será usado. Por exemplo: Uma gaveta com trimestres de Q1 a Q4 pode ter as seguintes atribuições: • Q1: Node_A_1 pool0 • Q2: Node_A_2 pool0 • Q3: Nó_B_1 pool1 • Q4:node_B_2 pool1 Metade das unidades internas permanecem sem atribuição antes de o MetroCluster ser configurado.	Cada um dos dois plexes no agregado raiz inclui as seguintes partições: • Duas partições para dados • Duas partições de paridade • Sem peças sobressalentes

ADP e atribuição de disco em sistemas AFF C250, AFF A250, ASA A250, ASA C250 e FAS500f

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz

Mínimo de unidades recomendadas (por local)	48 unidades	As unidades em cada compartimento externo são divididas em dois grupos iguais (metades). Cada meia prateleira é atribuída automaticamente a um pool separado.	Uma gaveta é usada pelo par de HA local. O segundo compartimento é usado pelo par de HA remoto. Partições em cada prateleira são usadas para criar o agregado raiz. O agregado raiz inclui as seguintes partições em cada Plex: • Oito partições para dados • Duas partições de paridade • Duas partições de reposição
Mínimo de unidades compatíveis (por local)	16 unidades internas	As unidades são divididas em quatro grupos iguais. Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexes no agregado raiz inclui as seguintes partições: • Duas partições para dados • Duas partições de paridade • Sem partições de reposição

ADP e atribuição de disco em sistemas AFF A300

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz

Mínimo de unidades recomendadas (por local)	48 unidades	As unidades em cada compartimento externo são divididas em dois grupos iguais (metades). Cada meia prateleira é atribuída automaticamente a um pool separado.	Uma gaveta é usada pelo par de HA local. O segundo compartimento é usado pelo par de HA remoto. Partições em cada prateleira são usadas para criar o agregado raiz. O agregado raiz inclui as seguintes partições em cada Plex: • Oito partições para dados • Duas partições de paridade • Duas partições de reposição
Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais. Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexes no agregado raiz inclui as seguintes partições: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

ADP e atribuição de disco em sistemas AFF C400, AFF A400, ASA C400 e ASA A400

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	96 unidades	As unidades são atribuídas automaticamente gaveta a gaveta.	Cada um dos dois plexos no agregado raiz inclui: • 20 partições para dados • Duas partições de paridade • Duas partições de reposição

Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais (trimestres). Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexos no agregado raiz inclui: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

ADP e atribuição de disco em sistemas AFF A700

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	96 unidades	As unidades são atribuídas automaticamente gaveta a gaveta.	Cada um dos dois plexos no agregado raiz inclui: • 20 partições para dados • Duas partições de paridade • Duas partições de reposição
Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais (trimestres). Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexos no agregado raiz inclui: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

ADP e atribuição de disco em sistemas AFF C800, ASA C800, ASA A800, AFF A800, AFF A70 e AFF A90

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para agregado de raiz

Mínimo de unidades recomendadas (por local)	Unidades internas e 96 unidades externas	As partições internas são divididas em quatro grupos iguais (trimestres). Cada trimestre é atribuído automaticamente a um pool separado. As unidades nas gavetas externas são atribuídas automaticamente a cada gaveta, com todas as unidades em cada gaveta atribuídas a um dos quatro nós da configuração MetroCluster.	O agregado raiz é criado com 12 partições raiz no compartimento interno. Cada um dos dois plexos no agregado raiz inclui: • Oito partições para dados • Duas partições de paridade • Duas partições de reposição
Mínimo de unidades compatíveis (por local)	24 unidades internas	As partições internas são divididas em quatro grupos iguais (trimestres). Cada trimestre é atribuído automaticamente a um pool separado.	O agregado raiz é criado com 12 partições raiz no compartimento interno. Cada um dos dois plexos no agregado raiz inclui: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

ADP e atribuição de disco em sistemas AFF A900, ASA A900 e AFF A1K

Diretriz	Compartimentos por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	96 unidades	As unidades são atribuídas automaticamente gaveta a gaveta.	Cada um dos dois plexos no agregado raiz inclui: • 20 partições para dados • Duas partições de paridade • Duas partições de reposição

Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais (trimestres). Cada compartimento é atribuído automaticamente a um pool separado.	Cada um dos dois plexos no agregado raiz inclui: • Três partições para dados • Duas partições de paridade • Uma partição sobressalente

Atribuição de disco em sistemas FAS2750

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	24 unidades internas e 24 unidades externas	As prateleiras internas e externas são divididas em duas metades iguais. Cada metade é atribuída automaticamente a um pool diferente	Não aplicável
Mínimo de unidades suportadas (por local) (configuração de HA ativa/passiva)	Apenas unidades internas	Atribuição manual necessária	Não aplicável

Atribuição de disco em sistemas FAS8200

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	48 unidades	As unidades nas prateleiras externas são divididas em dois grupos iguais (metades). Cada meia prateleira é atribuída automaticamente a um pool separado.	Não aplicável
Mínimo de unidades suportadas (por local) (configuração de HA ativa/passiva)	24 unidades	Atribuição manual necessária.	Não aplicável

Atribuição de disco em sistemas FAS500f

As mesmas diretrizes e regras de atribuição de disco para sistemas AFF C250 e AFF A250 se aplicam aos sistemas FAS500f. Para atribuição de discos em sistemas FAS500f, consulte a [ADP_FAS500f]tabela.

Atribuição de disco em sistemas FAS9000

Diretriz	Unidades por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	96 unidades	As unidades são atribuídas automaticamente gaveta a gaveta.	Não aplicável
Mínimo de unidades compatíveis (por local)	48 unidades	As unidades nas prateleiras são divididas em dois grupos iguais (metades). Cada meia prateleira é atribuída automaticamente a um pool separado.	Não aplicável

Atribuição de disco em sistemas FAS9500

Diretriz	Compartimentos por local	Regras de atribuição de unidades	Layout ADP para partição raiz
Mínimo de unidades recomendadas (por local)	96 unidades	As unidades são atribuídas automaticamente gaveta a gaveta.	Não aplicável
Mínimo de unidades compatíveis (por local)	24 unidades	As unidades são divididas em quatro grupos iguais (trimestres). Cada compartimento é atribuído automaticamente a um pool separado.	Não aplicável

Peering de clusters

Cada site do MetroCluster é configurado como um ponto do site do parceiro. Você deve estar familiarizado com os pré-requisitos e diretrizes para configurar as relações de peering. Isso é importante ao decidir se usar portas compartilhadas ou dedicadas para esses relacionamentos.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar que a conetividade entre os requisitos de porta, endereço IP, sub-rede, firewall e nomenclatura de cluster é atendida.

Requisitos de conetividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

  Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.

> O ONTAP 9 permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

  Você pode usar vários IPspaces para fazer pares com vários clusters. A conetividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

  As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Serviço ICMP
- TCP para os endereços IP de todos os LIFs entre clusters nas portas 10000, 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

A política de firewall entre clusters padrão permite o acesso através do protocolo HTTPS e de todos os

endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Considerações ao usar portas dedicadas

Ao determinar se o uso de uma porta dedicada para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alteração e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o uso de uma porta dedicada é a melhor solução de rede entre clusters:

- Se a quantidade de largura de banda da WAN disponível for semelhante à das portas LAN e o intervalo de replicação for tal que a replicação ocorra enquanto a atividade do cliente regular existe, você deve dedicar portas Ethernet para replicação entre clusters para evitar a contenção entre replicação e os protocolos de dados.
- Se a utilização da rede gerada pelos protocolos de dados (CIFS, NFS e iSCSI) for tal que a utilização da rede seja superior a 50%, dedique portas para replicação para permitir desempenho não degradado se ocorrer um failover de nó.
- Quando portas físicas de 10 GbE ou mais rápidas são usadas para dados e replicação, você pode criar portas VLAN para replicação e dedicar as portas lógicas para replicação entre clusters.

  A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.

Considerações ao compartilhar portas de dados

Ao determinar se o compartilhamento de uma porta de dados para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alterações e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o compartilhamento de portas de dados é a melhor solução de conetividade entre clusters:

- Para uma rede de alta velocidade, como uma rede 40-Gigabit Ethernet (40-GbE), uma quantidade suficiente de largura de banda local da LAN pode estar disponível para executar a replicação nas mesmas portas de 40 GbE que são usadas para acesso aos dados.

  Em muitos casos, a largura de banda da WAN disponível é muito menor do que a largura de banda da LAN de 10 GbE.

- Todos os nós no cluster podem ter que replicar dados e compartilhar a largura de banda da WAN disponível, tornando o compartilhamento da porta de dados mais aceitável.
- O compartilhamento de portas para dados e replicação elimina as contagens de portas extras necessárias para dedicar portas para replicação.
- O tamanho máximo da unidade de transmissão (MTU) da rede de replicação será o mesmo tamanho que o utilizado na rede de dados.
- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.

- Quando as portas de dados para replicação entre clusters são compartilhadas, as LIFs entre clusters podem ser migradas para qualquer outra porta compatível com clusters no mesmo nó para controlar a porta de dados específica usada para replicação.

Requisitos da ISL

Visão geral dos requisitos do ISL

Você deve verificar se a configuração e a rede IP do MetroCluster atendem a todos os requisitos de enlace interswitch (ISL). Embora certos requisitos possam não se aplicar à sua configuração, você ainda deve estar ciente de todos os requisitos do ISL para obter uma melhor compreensão da configuração geral.

A tabela a seguir fornece uma visão geral dos tópicos abordados nesta seção.

Título	Descrição
"Switches validados pela NetApp e compatíveis com MetroCluster"	Descreve os requisitos do interrutor. Aplica-se a todos os switches usados nas configurações do MetroCluster, incluindo switches de back-end.
"Considerações para ISLs"	Descreve os requisitos do ISL. Aplica-se a todas as configurações do MetroCluster, independentemente da topologia de rede e se você usa switches validados pela NetApp ou switches compatíveis com MetroCluster.
"Considerações ao implantar o MetroCluster em redes de camada 2 ou camada 3 compartilhadas"	Descreve os requisitos para redes de camada 2 ou camada 3 compartilhadas. Aplica-se a todas as configurações, exceto para configurações MetroCluster que usam switches validados pela NetApp e usando ISLs conetados diretamente.
"Considerações ao usar switches compatíveis com MetroCluster"	Descreve os requisitos para switches compatíveis com MetroCluster. Aplica-se a todas as configurações do MetroCluster que não estejam usando switches validados pela NetApp.
"Exemplos de topologias de rede MetroCluster"	Fornece exemplos de diferentes topologias de rede MetroCluster. Aplica-se a todas as configurações do MetroCluster.

Switches validados pela NetApp e compatíveis com MetroCluster

Todos os switches usados na configuração, incluindo os switches de back-end, precisam ser validados pela NetApp ou em conformidade com a MetroCluster.

Switches validados pela NetApp

Um switch é validado pela NetApp se atender aos seguintes requisitos:

- O switch é fornecido pelo NetApp como parte da configuração IP do MetroCluster
- O switch está listado no "NetApp Hardware Universe" como um switch suportado em *MetroCluster-over-IP-Connections*
- O switch só é usado para conectar controladores IP MetroCluster e, em algumas configurações, NS224 compartimentos de unidades
- O switch é configurado usando o arquivo de configuração de referência (RCF) fornecido pelo NetApp

Qualquer switch que não atenda a esses requisitos é **não** um switch validado pela NetApp.

Switches compatíveis com MetroCluster

Um switch compatível com MetroCluster não é validado pela NetApp, mas pode ser usado em uma configuração IP do MetroCluster se ele atender a certos requisitos e diretrizes de configuração.

> A NetApp não fornece serviços de solução de problemas ou suporte à configuração para qualquer switch não validado em conformidade com MetroCluster.

Considerações para ISLs

Links interswitches (ISLs) que transportam tráfego MetroCluster em todas as configurações IP do MetroCluster e topologias de rede têm certos requisitos. Esses requisitos se aplicam a todos os ISLs que transportam tráfego MetroCluster, independentemente de os ISLs serem diretos ou compartilhados entre os switches do cliente.

Requisitos gerais do MetroCluster ISL

O seguinte aplica-se a ISLs em todas as configurações IP do MetroCluster:

- Ambos os tecidos devem ter o mesmo número de ISLs.
- ISLs em um tecido devem ter a mesma velocidade e comprimento.
- Os ISLs em ambos os tecidos devem ter a mesma velocidade e comprimento.
- A diferença máxima suportada na distância entre o tecido 1 e o tecido 2 é 20km ou 0,2ms.
- Os ISLs devem ter a mesma topologia. Por exemplo, todos devem ser links diretos, ou se a configuração usa WDM, então todos devem usar WDM.
- A velocidade ISL deve ser, no mínimo, 10Gbps.
- Deve haver pelo menos um porto de 10Gbps ISL por tecido.

Limites de latência e perda de pacotes nos ISLs

O seguinte se aplica ao tráfego de ida e volta entre os switches IP MetroCluster no site_A e site_B, com a configuração MetroCluster em operação de estado estável:

- À medida que a distância entre dois locais de MetroCluster aumenta, a latência aumenta, geralmente no intervalo de 1 ms de tempo de atraso de ida e volta por 100 km (62 milhas). A latência também depende do acordo de nível de serviço de rede (SLA) em termos de largura de banda dos links ISL, taxa de queda de pacotes e jitter na rede. Baixa largura de banda, alta instabilidade e quedas aleatórias de pacotes levam a diferentes mecanismos de recuperação pelos switches, ou o mecanismo TCP nos módulos do controlador, para uma entrega de pacotes bem-sucedida. Esses mecanismos de recuperação podem aumentar a latência geral. Para obter informações específicas sobre a latência de ida e volta e os requisitos de distância máxima para a sua configuração, consulte a. "Hardware Universe."
- Qualquer dispositivo que contribua para a latência deve ser contabilizado.
- O "Hardware Universe." fornece a distância em km. Você deve alocar 1ms para cada 100km. A distância máxima é definida pelo que é atingido primeiro, seja o tempo máximo de ida e volta (RTT) em ms, ou a distância em km. Por exemplo, se *o Hardware Universe* indicar uma distância de 300km, traduzindo para 3ms, o seu ISL não pode ser mais do que 300km e o RTT máximo não pode exceder 3ms – o que for

atingido primeiro.

- A perda de pacotes deve ser inferior ou igual a 0,01%. A perda máxima de pacotes é a soma de todas as perdas em todos os links no caminho entre os nós MetroCluster e a perda nas interfaces IP MetroCluster locais.
- O valor de jitter suportado é 3ms para ida e volta (ou 1,5ms para ida e volta).
- A rede deve alocar e manter a quantidade de largura de banda SLA necessária para o tráfego MetroCluster, independentemente de microexplosões e picos no tráfego.
- Se você estiver usando o ONTAP 9.7 ou posterior, a rede intermediária entre os dois locais deve fornecer uma largura de banda mínima de 4,5Gbps Gbps para a configuração IP do MetroCluster.

Considerações sobre transcetor e cabo

Todos os SFPs ou QSFPs suportados pelo fornecedor de equipamentos são suportados para os ISLs da MetroCluster. Os SFPs e QSFPs fornecidos pela NetApp ou pelo fornecedor do equipamento devem ser suportados pelo firmware do switch e do switch.

Ao conetar os controladores aos switches e aos ISLs de cluster locais, você deve usar os transcetores e cabos fornecidos pela NetApp com o MetroCluster.

Quando você usa um adaptador QSFP-SFP, a configuração da porta no modo breakout ou velocidade nativa depende do modelo do switch e do firmware. Por exemplo, o uso de um adaptador QSFP-SFP com switches Cisco 9336C que executam o firmware NX-os 9.x ou 10.x requer que você configure a porta no modo de velocidade nativo.

Se configurar um RCF, verifique se seleciona o modo de velocidade correto ou se utiliza uma porta com um modo de velocidade adequado.

Usando xWDM, TDM e dispositivos de criptografia externos

Quando você usa dispositivos xWDM/TDM ou dispositivos que fornecem criptografia em uma configuração IP MetroCluster, seu ambiente deve atender aos seguintes requisitos:

- Ao conetar os switches IP MetroCluster ao xWDM/TDM, os dispositivos de criptografia externos ou o equipamento xWDM/TDM devem ser certificados pelo fornecedor para o switch e o firmware. A certificação deve abranger o modo operacional (como entroncamento e criptografia).
- A latência e o jitter totais de ponta a ponta, incluindo a criptografia, não podem ser maiores do que o valor máximo indicado no IMT e nesta documentação.

Número suportado de ISLs e cabos de arranque

A tabela a seguir mostra o número máximo suportado de ISLs que podem ser configuradas em um switch IP MetroCluster usando a configuração Arquivo de Configuração de Referência (RCF).

Modelo de switch IP MetroCluster	Tipo de porta	Número máximo de ISLs
Switches BES-53248 compatíveis com Broadcom	Portas nativas	4 ISLs usando 10Gbps ou 25Gbps
Switches BES-53248 compatíveis com Broadcom	Portas nativas (Nota 1)	2 ISLs usando 40Gbps ou 100Gbps

Cisco 3132Q-V	Portas nativas	6 ISLs usando 40Gbps
Cisco 3132Q-V	Cabos de arranque	16 ISLs usando 10Gbps
Cisco 3232C	Portas nativas	6 ISLs usando 40Gbps ou 100Gbps
Cisco 3232C	Cabos de arranque	16 ISLs usando 10Gbps ou 25Gbps
Cisco 9336C-FX2 (não conecta gavetas NS224)	Portas nativas	6 ISLs usando 40Gbps ou 100Gbps
Cisco 9336C-FX2 (não conecta gavetas NS224)	Cabos de arranque	16 ISLs usando 10Gbps ou 25Gbps
Cisco 9336C-FX2 (conexão de NS224 gavetas)	Portas nativas (Nota 2)	4 ISLs usando 40Gbps ou 100Gbps
Cisco 9336C-FX2 (conexão de NS224 gavetas)	Cabos de arranque (Nota 2)	16 ISLs usando 10Gbps ou 25Gbps
NVIDIA SN2100	Portas nativas (Nota 2)	2 ISLs usando 40Gbps ou 100Gbps
NVIDIA SN2100	Cabos de arranque (Nota 2)	8 ISLs usando 10Gbps ou 25Gbps

Nota 1: O uso de 40Gbps ou 100Gbps ISLs em um switch BES-53248 requer uma licença adicional.

Nota 2: As mesmas portas são usadas para velocidade nativa e modo de breakout. Você deve optar por usar portas no modo de velocidade nativa ou no modo de breakout ao criar o arquivo RCF.

- Todos os ISLs em um switch IP MetroCluster devem ter a mesma velocidade. O uso de uma combinação de portas ISL com diferentes velocidades simultaneamente não é suportado.
- Para um desempenho ideal, deve utilizar pelo menos um 40Gbps ISL por rede. Você não deve usar um único ISL 10Gbps por rede para FAS9000, AFF A700 ou outras plataformas de alta capacidade.

> A NetApp recomenda que você configure um pequeno número de ISLs de alta largura de banda, em vez de um alto número de ISLs de baixa largura de banda. Por exemplo, é preferível configurar um ISL 40Gbps em vez de quatro ISLs 10Gbps. Ao usar vários ISLs, o balanceamento de carga estatístico pode afetar o rendimento máximo. O balanceamento desigual pode reduzir o rendimento para o de um único ISL.

Considerações ao implantar o MetroCluster em redes compartilhadas da camada 2 ou da camada 3

Dependendo dos seus requisitos, você pode usar redes compartilhadas da camada 2 ou da camada 3 para implantar o MetroCluster.

A partir do ONTAP 9.6, as configurações IP do MetroCluster com switches suportados podem compartilhar redes existentes para links interswitches (ISLs) em vez de usar ISLs MetroCluster dedicados. Essa topologia é conhecida como *shared layer 2 networks*.

A partir do ONTAP 9.9,1, as configurações IP do MetroCluster podem ser implementadas com conexões de back-end roteadas por IP (camada 3). Essa topologia é conhecida como *shared layer 3 networks*.

- Nem todos os recursos são suportados em todas as topologias de rede.
- Você deve verificar se tem capacidade de rede adequada e se o tamanho ISL é apropriado para sua configuração. A baixa latência é essencial para a replicação de dados entre os locais do MetroCluster. Problemas de latência nessas conexões podem afetar a e/S do cliente
- Todas as referências a switches de back-end MetroCluster referem-se a switches validados por NetApp ou compatíveis com MetroCluster. "Switches validados pela NetApp e compatíveis com MetroCluster"Consulte para obter mais detalhes.

Requisitos de ISL para redes de camada 2 e camada 3

O seguinte se aplica às redes da camada 2 e da camada 3:

- A velocidade e o número de ISLs entre os switches MetroCluster e os switches de rede intermediários não precisam ser compatíveis. Da mesma forma, a velocidade entre os switches de rede intermediária não precisa corresponder.

  Por exemplo, os switches MetroCluster podem se conetar usando um 40Gbps ISL aos interrutores intermediários, e os interrutores intermediários podem se conetar usando dois ISLs de 100Gbps.

- O monitoramento de rede deve ser configurado na rede intermediária para monitorar os ISLs para utilização, erros (quedas, flaps de link, corrupção, etc.) e falhas.
- O tamanho da MTU deve ser definido como 9216 em todas as portas que transportam tráfego MetroCluster de ponta a ponta.
- Nenhum outro tráfego pode ser configurado com uma prioridade mais alta do que a classe de serviço (COS) 5.
- A notificação explícita de congestionamento (ECN) deve ser configurada em todos os caminhos que transportam tráfego MetroCluster de ponta a ponta.
- Os ISLs que transportam tráfego MetroCluster devem ser links nativos entre os switches.

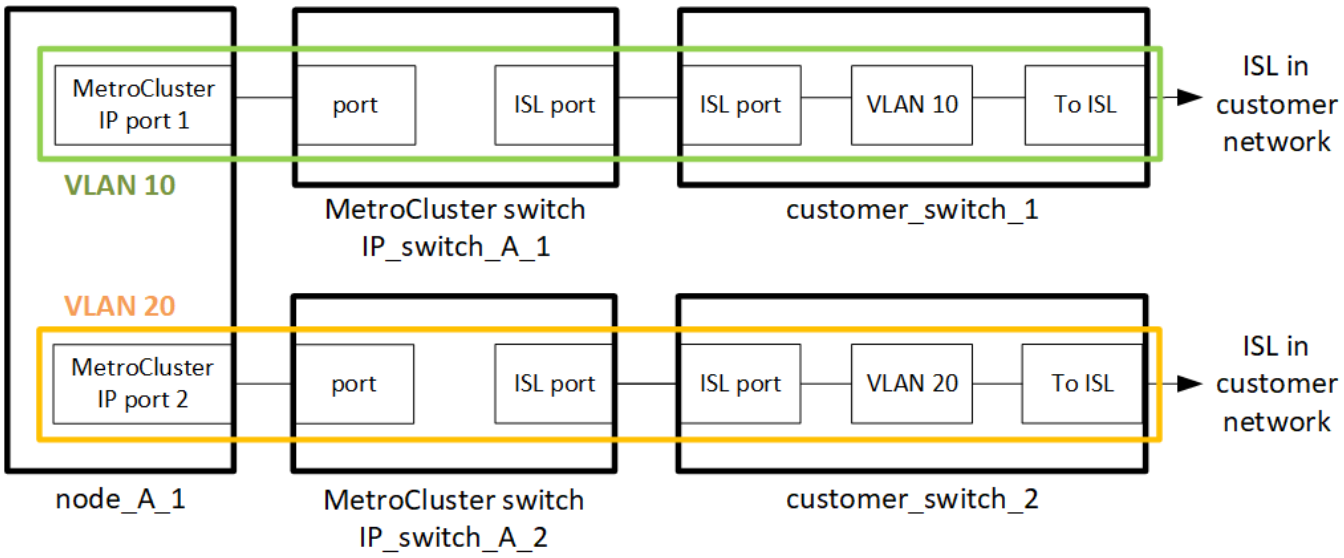
  Os serviços de compartilhamento de links, como os links MPLS (Multiprotocol Label Switching), não são suportados.

- As VLANs de camada 2 devem abranger nativamente os locais. A sobreposição de VLAN, como a Virtual Extensible LAN (VXLAN), não é suportada.
- O número de interrutores intermédios não é limitado. No entanto, a NetApp recomenda que você mantenha o número de switches ao mínimo necessário.
- Os ISLs nos switches MetroCluster são configurados com o seguinte:
  - Modo de porta do switch 'trunk' como parte de um canal de porta LACP
  - O tamanho da MTU é 9216
  - Nenhuma VLAN nativa está configurada
  - Somente VLANs que transportam tráfego MetroCluster entre locais são permitidas

◦ A VLAN padrão do switch não é permitida

Considerações para redes de camada 2

Os switches de back-end MetroCluster são conetados à rede do cliente.



Os interrutores intermediários fornecidos pelo cliente devem cumprir os seguintes requisitos:

- A rede intermediária deve fornecer as mesmas VLANs entre os locais. Isso deve corresponder às VLANs MetroCluster definidas no arquivo RCF.
- O RcfFileGenerator não permite a criação de um arquivo RCF usando VLANs que não são suportadas pela plataforma.
- O RcfFileGenerator pode restringir o uso de certos IDs de VLAN, por exemplo, se eles são destinados para uso futuro. Geralmente, as VLANs reservadas são até 100.1X, inclusive.
- As VLANs de camada 2 com IDs que correspondam às IDs de VLAN MetroCluster devem abranger a rede compartilhada.

Configuração de VLAN no ONTAP

Você só pode especificar a VLAN durante a criação da interface. Você pode configurar as VLANs padrão 10 e 20 ou VLANs dentro do intervalo de 101 a 4096 (ou o número suportado pelo fornecedor do switch, o que for o número menor). Depois que as interfaces MetroCluster forem criadas, você não poderá alterar o ID da VLAN.

Alguns fornecedores de switches podem reservar o uso de certas VLANs.

Os sistemas a seguir não exigem configuração de VLAN no ONTAP. A VLAN é especificada pela configuração da porta do switch:

- FAS8200 e AFF A300
- AFF A320
- FAS9000 e AFF A700
- AFF A800, ASA A800, AFF C800 e ASA C800

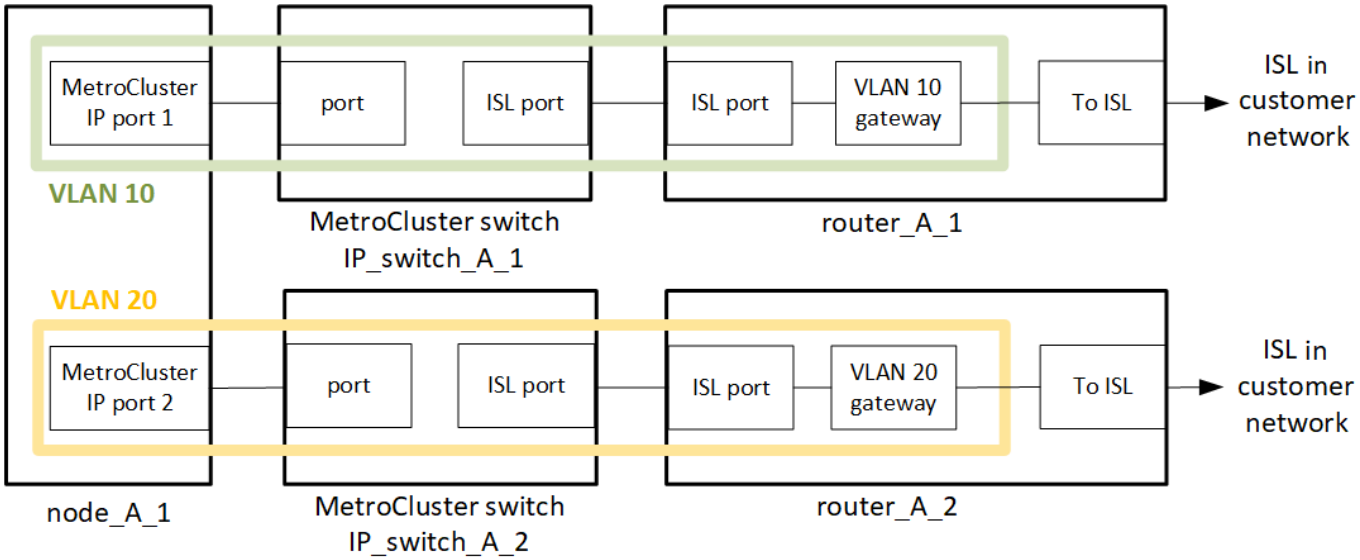
Os sistemas listados acima podem ser configurados usando VLANs 100 e abaixo. No entanto, algumas VLANs nesse intervalo podem ser reservadas para uso futuro ou outro.

Para todos os outros sistemas, você deve configurar a VLAN ao criar as interfaces MetroCluster no ONTAP. Aplicam-se as seguintes restrições:

- A VLAN padrão é 10 e 20
- Se você estiver executando o ONTAP 9.7 ou anterior, você só poderá usar a VLAN 10 e 20 padrão.
- Se você estiver executando o ONTAP 9.8 ou posterior, você pode usar a VLAN 10 e 20 padrão e uma VLAN acima de 100 (101 e superior) também pode ser usada.

Considerações para redes de camada 3

Os switches de back-end MetroCluster são conetados à rede IP roteada, diretamente aos roteadores (como mostrado no exemplo simplificado a seguir) ou por meio de outros switches intervenientes.



O ambiente MetroCluster é configurado e cabeado como uma configuração IP MetroCluster padrão, conforme descrito em "Configure os componentes de hardware do MetroCluster". Ao executar o procedimento de instalação e cabeamento, você deve executar as etapas específicas de uma configuração de camada 3. O seguinte se aplica às configurações da camada 3:

- Você pode conetar switches MetroCluster diretamente ao roteador ou a um ou mais switches intervenientes.
- Você pode conetar interfaces IP MetroCluster diretamente ao roteador ou a um dos switches intervenientes.
- A VLAN deve ser estendida ao dispositivo de gateway.
- Utilize o `-gateway parameter` para configurar o endereço de interface IP do MetroCluster com um endereço de gateway IP.
- Os IDs de VLAN para as VLANs MetroCluster devem ser os mesmos em cada local. No entanto, as sub-redes podem ser diferentes.
- O roteamento dinâmico não é suportado para o tráfego MetroCluster.
- Os seguintes recursos não são suportados:

- Configurações de MetroCluster de oito nós
- Atualizando uma configuração de MetroCluster de quatro nós
- Transição do MetroCluster FC para o MetroCluster IP

- São necessárias duas sub-redes em cada local do MetroCluster, uma em cada rede.
- A atribuição Auto-IP não é suportada.

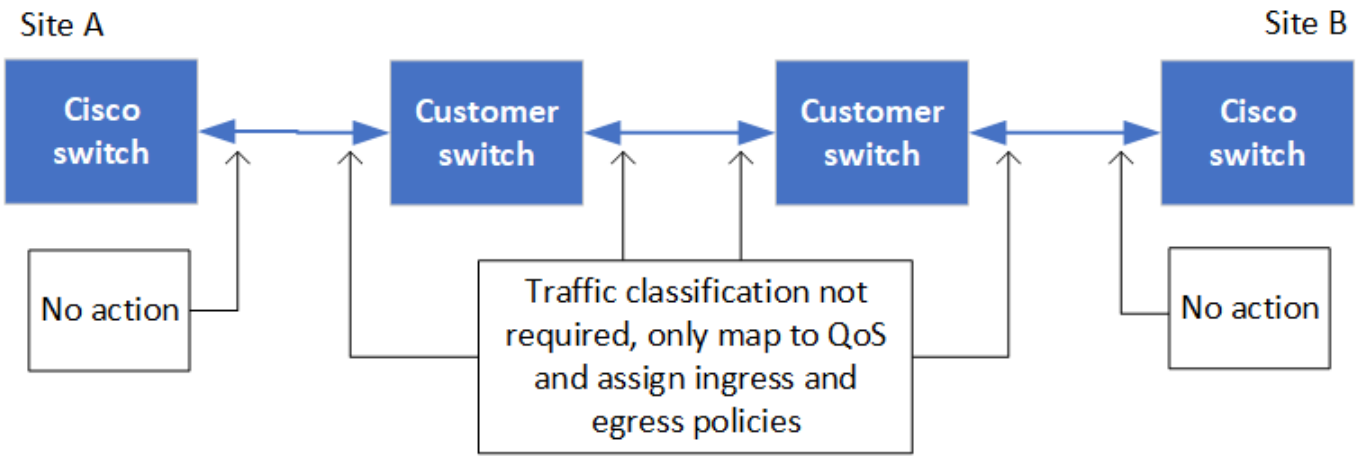
Ao configurar roteadores e endereços IP de gateway, você deve atender aos seguintes requisitos:

- Duas interfaces em um nó não podem ter o mesmo endereço IP de gateway.
- As interfaces correspondentes nos pares de HA em cada local devem ter o mesmo endereço IP de gateway.
- As interfaces correspondentes em um nó e seus parceiros DR e AUX não podem ter o mesmo endereço IP de gateway.
- As interfaces correspondentes em um nó e seus parceiros DR e AUX devem ter o mesmo ID VLAN.

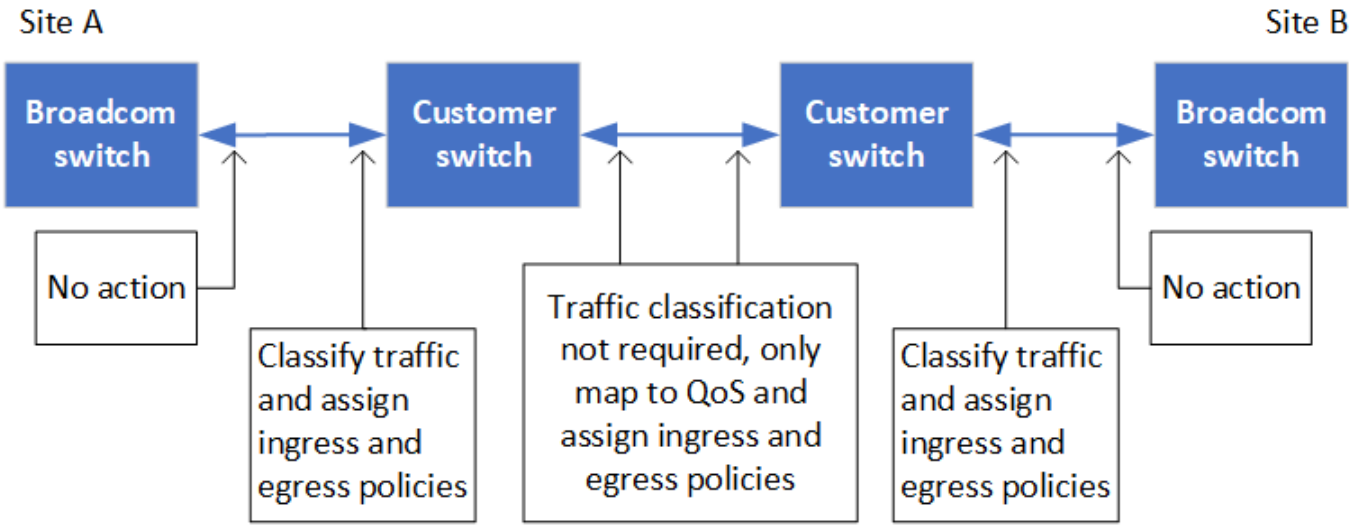
Definições necessárias para interrutores intermédios

Quando o tráfego MetroCluster atravessa um ISL em uma rede intermediária, você deve verificar se a configuração dos switches intermediários garante que o tráfego MetroCluster (RDMA e armazenamento) atenda aos níveis de serviço necessários em todo o caminho entre os locais do MetroCluster.

O diagrama a seguir fornece uma visão geral das configurações necessárias ao usar switches Cisco validados da NetApp:



O diagrama a seguir apresenta uma visão geral das configurações necessárias para uma rede compartilhada quando os switches externos são switches IP Broadcom.



Neste exemplo, as seguintes políticas e mapas são criados para o tráfego MetroCluster:

- A `MetroClusterIP_ISL_Ingress` política é aplicada a portas no switch intermediário que se coneta aos switches IP MetroCluster.

  A `MetroClusterIP_ISL_Ingress` política mapeia o tráfego marcado de entrada para a fila apropriada no switch intermediário.

- Uma `MetroClusterIP_ISL_Egress` política é aplicada a portas no switch intermediário que se conetam a ISLs entre switches intermediários.
- Você deve configurar as centrais intermediárias com mapas de acesso QoS correspondentes, mapas de classe e mapas de políticas ao longo do caminho entre os switches IP MetroCluster. Os switches intermediários mapeiam o tráfego RDMA para COS5 e o tráfego de armazenamento para COS4.

Os exemplos a seguir são para os switches Cisco Nexus 3232C e 9336C-FX2. Dependendo do fornecedor e do modelo do switch, você deve verificar se os switches intermediários têm uma configuração apropriada.

Configure o mapa de classe para a porta ISL do interrutor intermediário

O exemplo a seguir mostra as definições do mapa de classes, dependendo se você precisa classificar ou corresponder o tráfego na entrada.

Classificar o tráfego na entrada:

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

Correspondência de tráfego no ingresso:

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

Crie um mapa de políticas de entrada na porta ISL do switch intermediário:

Os exemplos a seguir mostram como criar um mapa de políticas de ingresso, dependendo se você precisa classificar ou corresponder o tráfego no ingresso.

Classifique o tráfego no ingresso:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Faça corresponder o tráfego no ingresso:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Configure a política de enfileiramento de saída para as portas ISL

O exemplo a seguir mostra como configurar a política de enfileiramento de saída:

```
policy-map type queuing MetroClusterIP_ISL_Egress
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2
   class type queuing c-out-8q-q5
      priority level 3
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q4
      priority level 4
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q3
      priority level 5
   class type queuing c-out-8q-q2
      priority level 6
   class type queuing c-out-8q-q1
      priority level 7
   class type queuing c-out-8q-q-default
      bandwidth remaining percent 100
      random-detect threshold burst-optimized ecn
```

Estas definições têm de ser aplicadas em todos os interrutores e ISLs que transportam tráfego MetroCluster.

Neste exemplo, Q4 e Q5 são configurados com `random-detect threshold burst-optimized ecn`. Dependendo da configuração, talvez seja necessário definir os limites mínimo e máximo, como mostrado no exemplo a seguir:

```
class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
kbytes drop-probability 0 weight 0 ecn
```

Os valores mínimo e máximo variam de acordo com o switch e seus requisitos.

Exemplo 1: Cisco

Se sua configuração tiver switches Cisco, você não precisará classificar na primeira porta de entrada do switch intermediário. Em seguida, configure os seguintes mapas e políticas:

- `class-map type qos match-any c5`
- `class-map type qos match-any c4`

- `MetroClusterIP_ISL_Ingress_Match`

Atribua o `MetroClusterIP_ISL_Ingress_Match` mapa de políticas às portas ISL que transportam tráfego MetroCluster.

Exemplo 2: Broadcom

Se sua configuração tiver switches Broadcom, você deve classificar na primeira porta de entrada do switch intermediário. Em seguida, configure os seguintes mapas e políticas:

- `ip access-list rdma`
- `ip access-list storage`
- `class-map type qos match-all rdma`
- `class-map type qos match-all storage`
- `MetroClusterIP_ISL_Ingress_Classify`
- `MetroClusterIP_ISL_Ingress_Match`

Você atribui `the MetroClusterIP_ISL_Ingress_Classify` o mapa de políticas às portas ISL no switch intermediário que coneta o switch Broadcom.

Você atribui o `MetroClusterIP_ISL_Ingress_Match` mapa de políticas às portas ISL no switch intermediário que está transportando tráfego MetroCluster, mas não coneta o switch Broadcom.

Exemplos de topologias de rede MetroCluster

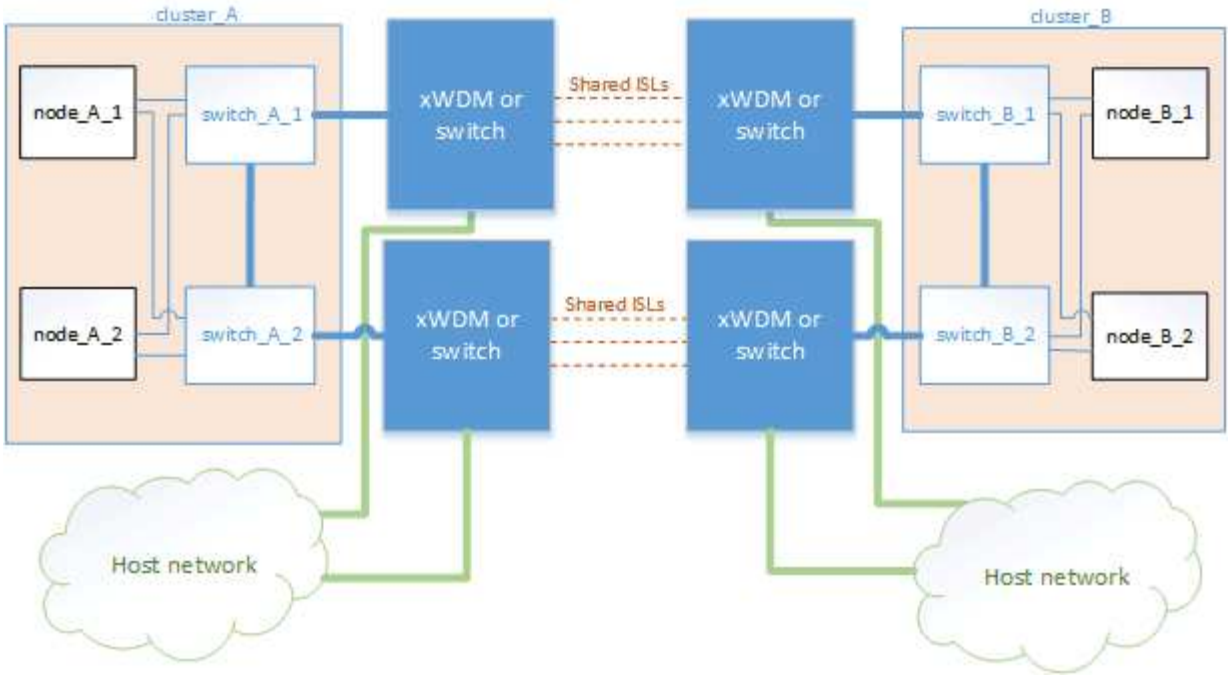
A partir do ONTAP 9.6, algumas configurações de rede adicionais são suportadas para configurações IP do MetroCluster. Esta seção fornece alguns exemplos das configurações de rede suportadas. Nem todas as topologias suportadas estão listadas.

Nestas topologias, assume-se que a rede ISL e intermédia são configuradas de acordo com os requisitos descritos na "Considerações para ISLs".

> Se você estiver compartilhando um ISL com tráfego não MetroCluster, verifique se o MetroCluster tem pelo menos a largura de banda mínima necessária disponível em todos os momentos.

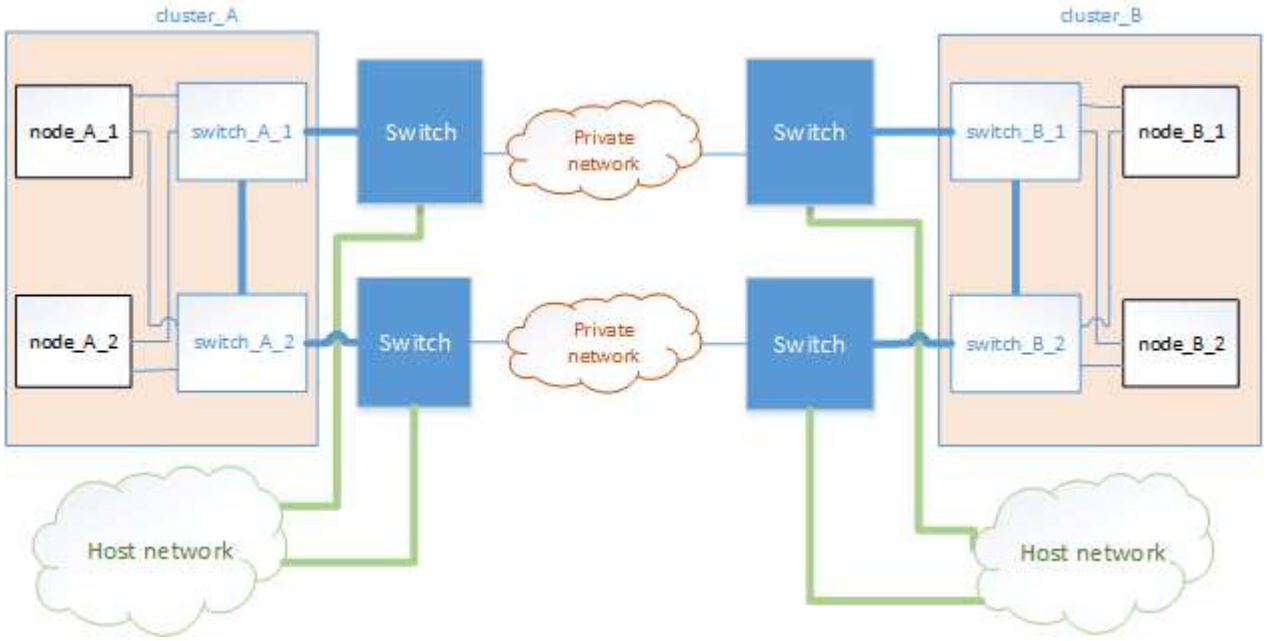
Configuração de rede compartilhada com links diretos

Nesta topologia, dois locais distintos são conetados por links diretos. Esses links podem ser entre dispositivos ou switches xWDM e TDM. A capacidade dos ISLs não é dedicada ao tráfego MetroCluster, mas é compartilhada com outro tráfego que não seja MetroCluster.



Infraestrutura compartilhada com redes intermediárias

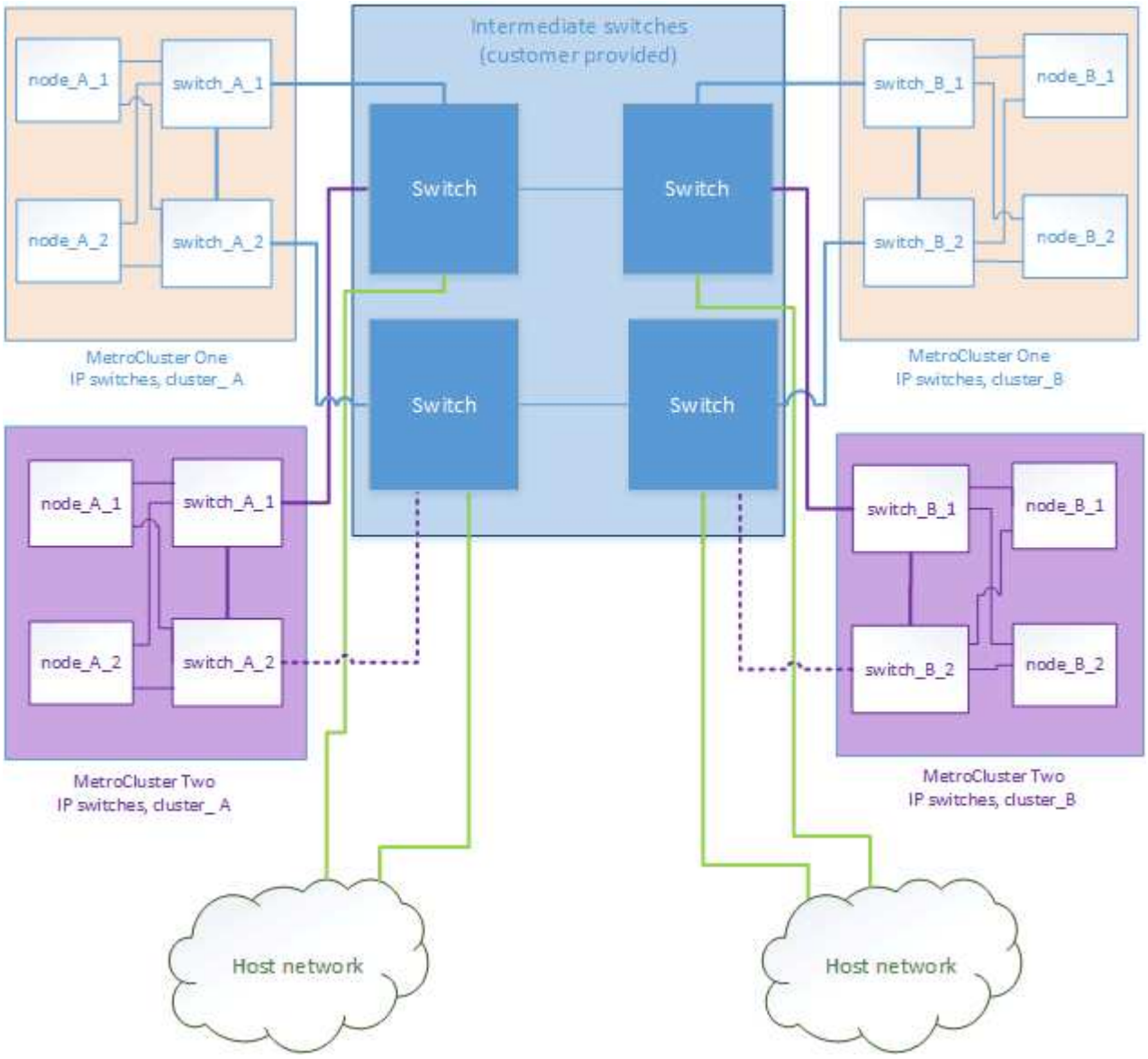
Nessa topologia, os sites do MetroCluster não são conetados diretamente, mas o MetroCluster e o tráfego do host viajam por uma rede. A rede pode consistir em uma série de xWDM e TDM e switches, mas ao contrário da configuração compartilhada com ISLs diretas, os links não são diretos entre os sites. Dependendo da infraestrutura entre os sites, qualquer combinação de configurações de rede é possível.



Várias configurações do MetroCluster compartilhando uma rede intermediária

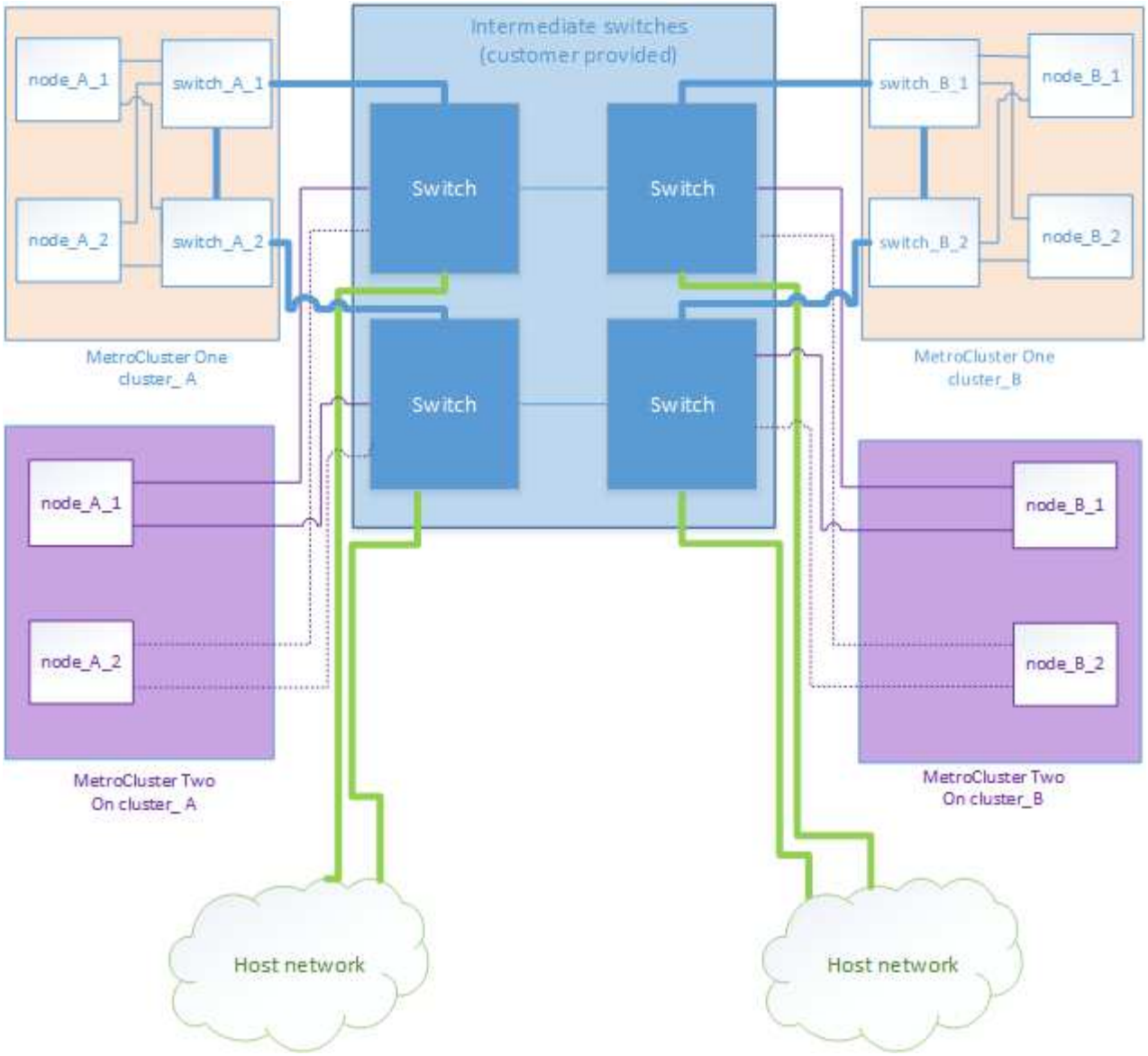
Nesta topologia, duas configurações MetroCluster separadas estão compartilhando a mesma rede intermediária. No exemplo, MetroCluster One switch_A_1 e MetroCluster two switch_A_1, ambos se conetam ao mesmo interrutor intermediário.

Ambas as configurações "MetroCluster One" ou "MetroCluster Two" podem ser de um MetroCluster de oito nós ou duas configurações de MetroCluster de quatro nós.



Combinação de uma configuração MetroCluster usando switches validados pela NetApp e uma configuração usando switches compatíveis com MetroCluster

Duas configurações MetroCluster separadas compartilham o mesmo switch intermediário, onde um MetroCluster é configurado usando switches validados NetApp em uma configuração de camada compartilhada 2 (MetroCluster One), e o outro MetroCluster é configurado usando switches compatíveis com MetroCluster conetando diretamente aos switches intermediários (MetroCluster Two).



Considerações para usar switches compatíveis com MetroCluster

Requisitos e limitações ao usar switches compatíveis com MetroCluster

A partir do ONTAP 9.7, as configurações IP do MetroCluster podem usar switches compatíveis com MetroCluster. Esses são switches que não são validados pela NetApp, mas estão em conformidade com as especificações da NetApp. No entanto, o NetApp não fornece serviços de suporte para solução de problemas ou configuração para nenhum switch não validado. Você deve estar ciente dos requisitos gerais e limitações ao usar switches compatíveis com MetroCluster.

Switches compatíveis com MetroCluster versus switches validados por NetApp

Um switch é validado pela NetApp se atender aos seguintes requisitos:

- O switch é fornecido pelo NetApp como parte da configuração IP do MetroCluster
- O switch está listado no "NetApp Hardware Universe" como um switch suportado em *MetroCluster-over-*

IP-Connections

- O switch só é usado para conectar controladores IP MetroCluster e, em algumas configurações, NS224 compartimentos de unidades
- O switch é configurado usando o arquivo de configuração de referência (RCF) fornecido pelo NetApp

Qualquer switch que não atenda a esses requisitos é **não** um switch validado pela NetApp.

Um switch compatível com MetroCluster não é validado pela NetApp, mas pode ser usado em uma configuração IP do MetroCluster se ele atender a certos requisitos e diretrizes de configuração.

> A NetApp não fornece serviços de solução de problemas ou suporte à configuração para qualquer switch não validado em conformidade com MetroCluster.

Requisitos gerais para switches compatíveis com MetroCluster

O switch que coneta as interfaces IP MetroCluster deve atender aos seguintes requisitos gerais:

- Os switches devem suportar qualidade de serviço (QoS) e classificação de tráfego.
- Os switches devem suportar notificação explícita de congestionamento (ECN).
- Os switches devem oferecer suporte a uma política de balanceamento de carga para preservar a ordem ao longo do caminho.
- Os interrutores devem suportar o Controle de fluxo L2 (L2FC).
- A porta do switch deve fornecer uma taxa dedicada e não deve ser superalocada.
- Os cabos e transcetores que conetam os nós aos switches devem ser fornecidos pela NetApp. Esses cabos devem ser suportados pelo fornecedor do switch. Se você estiver usando cabeamento ótico, o transcetor no switch pode não ser fornecido pelo NetApp. Você deve verificar se ele é compatível com o transcetor no controlador.
- Os switches que conetam os nós MetroCluster podem transportar tráfego não MetroCluster.
- Somente plataformas que fornecem portas dedicadas para interconexões de cluster sem switch podem ser usadas com um switch compatível com MetroCluster. Plataformas como o FAS2750 e o AFF A220 não podem ser usadas porque o tráfego MetroCluster e o tráfego de interconexão MetroCluster compartilham as mesmas portas de rede.
- O comutador compatível com MetroCluster não deve ser utilizado para ligações de cluster locais.
- A interface IP MetroCluster pode ser conetada a qualquer porta de switch que possa ser configurada para atender aos requisitos.
- São necessários quatro switches IP, dois para cada malha de switch. Se você usa diretores, então você pode usar um único diretor em cada lado, mas as interfaces IP do MetroCluster devem se conetar a dois blades diferentes em dois domínios de falha diferentes nesse diretor.
- As interfaces MetroCluster de um nó devem se conetar a dois switches de rede ou blades. As interfaces MetroCluster de um nó não podem ser conetadas à mesma rede ou switch ou blade.
- A rede deve atender aos requisitos descritos nas seções a seguir:
  - "Considerações para ISLs"
  - "Considerações ao implantar o MetroCluster em redes compartilhadas da camada 2 ou da camada 3"
- A unidade de transmissão máxima (MTU) de 9216 deve ser configurada em todos os interrutores que transportam tráfego IP MetroCluster.
- Reverter para o ONTAP 9.6 ou anterior não é suportado.

Todos os switches intermediários que você usar entre os switches que conetam as interfaces IP do MetroCluster em ambos os locais devem atender aos requisitos e ser configurados conforme descrito em "Considerações ao implantar o MetroCluster em redes compartilhadas da camada 2 ou da camada 3".

Limitações ao usar switches compatíveis com MetroCluster

Não é possível usar qualquer configuração ou recurso que exija que as conexões de cluster local estejam conetadas a um switch. Por exemplo, você não pode usar as seguintes configurações e procedimentos com um switch compatível com MetroCluster:

- Configurações de MetroCluster de oito nós
- Transição das configurações MetroCluster FC para MetroCluster IP
- Atualizando uma configuração de IP MetroCluster de quatro nós
- Plataformas que compartilham uma interface física para cluster local e tráfego MetroCluster. "Velocidades de rede específicas da plataforma e modos de porta de switch para switches compatíveis com MetroCluster"Consulte para obter informações sobre as velocidades suportadas.

Velocidades de rede específicas da plataforma e modos de porta de switch para switches compatíveis com MetroCluster

Se você estiver usando switches compatíveis com MetroCluster, deve estar ciente das velocidades de rede específicas da plataforma e dos requisitos do modo de porta do switch.

A tabela a seguir fornece velocidades de rede específicas da plataforma e modos de porta de switch para switches compatíveis com MetroCluster. Você deve configurar o modo de porta do switch de acordo com a tabela.

Valores ausentes indicam que a plataforma não pode ser usada com um switch compatível com MetroCluster.

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-
AFF A70	100Gbps	trunk mode
AFF A90	100Gbps	trunk mode
AFF A1K	100Gbps	trunk mode

Exemplos de configuração da porta do switch

Saiba mais sobre as várias configurações de portas do switch.

Os exemplos a seguir usam valores decimais e seguem a tabela que se aplica às centrais Cisco. Dependendo do fornecedor do switch, você pode exigir valores diferentes para DSCP. Consulte a tabela correspondente para o fornecedor do switch para confirmar o valor correto.

Valor DSCP	Decimal	Sextavado	Significado
101 000	16	0x10	CS2
011 000	24	0x18	CS3

100 000	32	0x20	CS4
101 000	40	0x28	CS5

Porta do switch que coneta uma interface MetroCluster

- Classificação para tráfego de acesso remoto à memória direta (RDMA):
  - Correspondência : porta TCP 10006, origem, destino ou ambos
  - Correspondência opcional: COS 5
  - Correspondência opcional: DSCP 40
  - Defina DSCP 40
  - Defina COS 5
  - Opcional : modelagem de taxa para 20Gbps
- Classificação para tráfego iSCSI:
  - Correspondência : porta TCP 62500, origem, destino ou ambos
  - Correspondência opcional: COS 4
  - Correspondência opcional: DSCP 32
  - Defina DSCP 32
  - Defina COS 4
- L2FlowControl (pausa), RX e TX

Portas ISL

- Classificação:
  - Combine COS 5 ou DSCP 40
    - Defina DSCP 40
    - Defina COS 5
  - Combine COS 4 ou DSCP 32
    - Defina DSCP 32
    - Defina COS 4
- Fila de saída
  - O grupo COS 4 tem um limite mínimo de configuração de 2000 e um limite máximo de 3000
  - O grupo COS 5 tem um limite mínimo de configuração de 3500 e um limite máximo de 6500.

    Os limites de configuração podem variar dependendo do ambiente. Você deve avaliar os limites de configuração com base em seu ambiente individual.

  - ECN ativado para Q4 e Q5
  - VERMELHO ativado para Q4 e Q5

Alocação de largura de banda (portas de switch que conetam interfaces MetroCluster e portas ISL)

- RDMA, COS 5 / DSCP 40: 60%

- ISCSI, COS 4 / DSCP 32: 40%
- Requisito mínimo de capacidade por configuração e rede do MetroCluster: 10Gbps

Se você usar limites de taxa, o tráfego deve ser **moldado** sem introduzir perdas.

Exemplos de configuração de portas de switch que conetam o controlador MetroCluster

Os comandos de exemplo fornecidos são válidos para as centrais Cisco NX3232 ou Cisco NX9336. Os comandos variam de acordo com o tipo de interrutor.

Se um recurso ou seu equivalente mostrado nos exemplos não estiver disponível no switch, o switch não atende aos requisitos mínimos e não pode ser usado para implantar uma configuração do MetroCluster. Isto é verdade para qualquer switch que se coneta a uma configuração MetroCluster e para todos os switches intermediários.

Os exemplos a seguir podem mostrar somente a configuração de uma rede.

Configuração básica

Uma LAN virtual (VLAN) em cada rede deve ser configurada. O exemplo a seguir mostra como configurar uma VLAN na rede 10.

Exemplo:

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

Exemplo:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

Exemplos para configurar a classificação

Você deve configurar mapas de acesso e classe para mapear o tráfego RDMA e iSCSI para as classes apropriadas.

No exemplo a seguir, todo o tráfego TCP de e para a porta 65200 é mapeado para a classe de armazenamento (iSCSI). Todo o tráfego TCP de e para a porta 10006 é mapeado para a classe RDMA. Esses mapas de políticas são usados em portas de switch que conetam as interfaces MetroCluster.

Exemplo:

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
match access-group name rdma
```

Tem de configurar uma política de entrada. Uma política de entrada mapeia o tráfego como classificado para diferentes grupos COS. Neste exemplo, o tráfego RDMA é mapeado para o grupo COS 5 e o tráfego iSCSI é mapeado para o grupo COS 4. A política de entrada é utilizada em portas de switch que ligam as interfaces MetroCluster e nas portas ISL que transportam tráfego MetroCluster.

Exemplo:

```
policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

A NetApp recomenda que você molda o tráfego em portas de switch conetando uma interface MetroCluster, como mostrado no exemplo a seguir:

Exemplo:

```
policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn
```

Exemplos para configurar as portas do nó

Talvez seja necessário configurar uma porta de nó no modo de breakout. No exemplo a seguir, as portas 25 e 26 são configuradas no modo de breakout 4 x 25Gbps.

Exemplo:

```
interface breakout module 1 port 25-26 map 25g-4x
```

Talvez seja necessário configurar a velocidade da porta da interface do MetroCluster. O exemplo a seguir mostra como configurar a velocidade para **auto** ou para o modo 40Gbps:

Exemplo:

```
    speed auto

    speed 40000
```

O exemplo a seguir mostra uma porta de switch configurada para conetar uma interface MetroCluster. É uma porta de modo de acesso na VLAN 10, com um MTU de 9216 e está operando em velocidade nativa. Ele tem controle de fluxo simétrico (enviar e receber) (pausa) ativado e as políticas de entrada e saída de MetroCluster atribuídas.

Exemplo:

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown
```

Nas portas 25Gbps, pode ser necessário definir a definição Correção de erro de Avanço (FEC) como "Off" (Desligado), conforme mostrado no exemplo a seguir.

Exemplo:

```
fec off
```

Exemplos de configuração de portas ISL em toda a rede

Um switch compatível com MetroCluster é considerado como um switch intermediário, mesmo ele coneta diretamente as interfaces MetroCluster. As portas ISL que transportam tráfego MetroCluster no switch compatível com MetroCluster devem ser configuradas da mesma forma que as portas ISL em um switch intermediário. "Definições necessárias nos interrutores intermédios"Consulte para obter orientações e exemplos.

Alguns mapas de políticas são os mesmos para portas de switch que conetam interfaces MetroCluster e ISLs que transportam tráfego MetroCluster. Você pode usar o mesmo mapa de políticas para ambos os usos de portas.

Usando agregados sem espelhamento

Se a sua configuração incluir agregados sem espelhamento, você precisa estar ciente de possíveis problemas de acesso após as operações de switchover.

Considerações para agregados sem espelhamento e namespaces hierárquicos

Se você estiver usando namespaces hierárquicos, você deve configurar o caminho de junção para que todos os volumes nesse caminho estejam apenas em agregados espelhados ou apenas em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados no caminho de junção pode impedir o acesso aos agregados sem espelhamento após a operação de comutação.

Considerações para agregados sem espelhamento e volumes de metadados CRS e volumes raiz de dados SVM

O volume de metadados do serviço de replicação de configuração (CRS) e os volumes raiz de dados do SVM devem estar em um agregado espelhado. Não é possível mover esses volumes para agregado sem espelhamento. Se eles estiverem em operações de comutação e switchback negociadas sem espelhamento, serão vetadas. O comando MetroCluster check fornece um aviso se for esse o caso.

Considerações para agregados sem espelhamento e SVMs

Os SVMs devem ser configurados somente em agregados espelhados ou somente em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados pode resultar em uma operação de switchover que excede 120 segundos e resultar em uma interrupção de dados se os agregados sem espelhamento não ficarem online.

Considerações para agregados sem espelhamento e SAN

Antes do ONTAP 9.9,1, um LUN não deve ser localizado em um agregado sem espelhamento. Configurar um LUN em um agregado sem espelhamento pode resultar em uma operação de switchover que excede 120 segundos e uma interrupção de dados.

Considerações para adicionar compartimentos de storage para agregados sem espelhamento

Se você estiver adicionando gavetas que serão usadas para agregados sem espelhamento em uma configuração MetroCluster IP, faça o seguinte:

1. Antes de iniciar o procedimento para adicionar as prateleiras, execute o seguinte comando:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Verifique se a atribuição automática de disco está desativada:

   ```
   disk option show
   ```

3. Siga os passos do procedimento para adicionar a prateleira.
4. Atribua manualmente todos os discos da nova gaveta ao nó que possuirá o agregado sem espelhamento ou agregados.
5. Crie os agregados:

   ```
   storage aggregate create
   ```

6. Depois de concluir o procedimento, execute o seguinte comando:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

7. Verifique se a atribuição automática de disco está ativada:

   ```
   disk option show
   ```

Uso de firewall em sites da MetroCluster

Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o

acesso a determinadas portas necessárias.

Considerações sobre o uso de firewall em sites da MetroCluster

Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o acesso às portas necessárias.

A tabela a seguir mostra o uso da porta TCP/UDP em um firewall externo posicionado entre dois sites do MetroCluster.

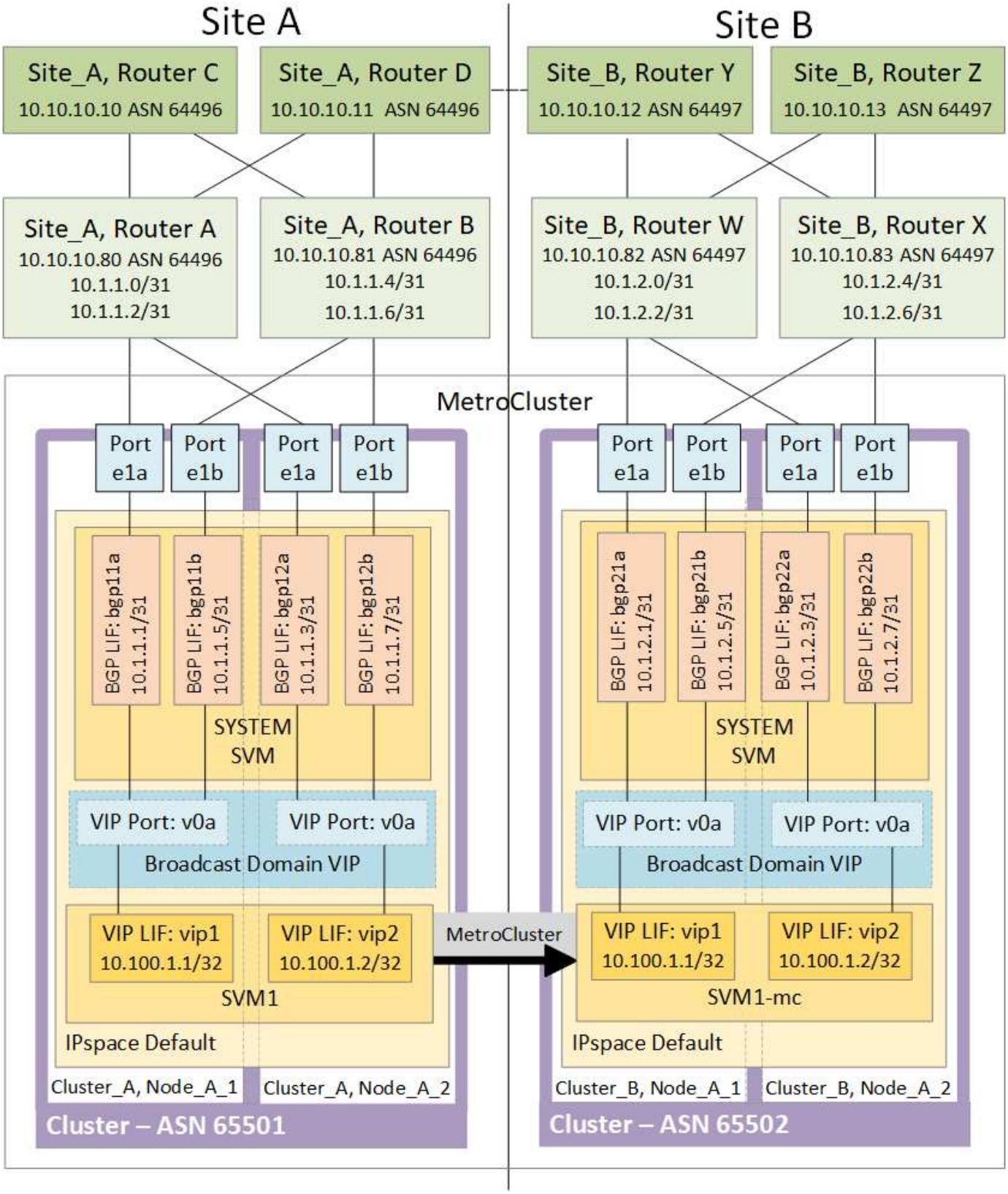
Tipo de trânsito	Porta/serviços
Peering de clusters	11104 / TCP 11105 / TCP
Gerente do sistema da ONTAP	443 / TCP
LIFs IP entre clusters do MetroCluster	65200 / TCP 10006 / TCP e UDP
Assistência ao hardware	4444 / TCP

Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster

A partir do ONTAP 9.5, o ONTAP oferece suporte à conetividade da camada 3 usando IP virtual (VIP) e protocolo de gateway de borda (BGP). A combinação VIP e BGP para redundância na rede front-end com a redundância MetroCluster back-end fornece uma solução de recuperação de desastres de camada 3.

Revise as diretrizes e a ilustração a seguir ao Planejar sua solução de camada 3. Para obter detalhes sobre como implementar o VIP e o BGP no ONTAP, consulte a seguinte seção:

"Configurando LIFs de IP virtual (VIP)"



Limitações do ONTAP

O ONTAP não verifica automaticamente se todos os nós em ambos os sites da configuração do MetroCluster estão configurados com peering BGP.

O ONTAP não executa agregação de rotas, mas anuncia todos os IPs de LIF virtuais individuais como rotas

de host exclusivas em todos os momentos.

O ONTAP não suporta True anycast — apenas um único nó no cluster apresenta um IP de LIF virtual específico (mas é aceito por todas as interfaces físicas, independentemente de serem LIFs BGP, desde que a porta física faça parte do espaço IPspace correto). Diferentes LIFs podem migrar independentemente um do outro para diferentes nós de hospedagem.

Diretrizes para usar esta solução de camada 3 com uma configuração MetroCluster

Você deve configurar seu BGP e VIP corretamente para fornecer a redundância necessária.

Cenários de implantação mais simples são preferidos em relação a arquiteturas mais complexas (por exemplo, um roteador de peering BGP é acessível em um roteador intermediário não BGP). No entanto, o ONTAP não aplica restrições de design ou topologia de rede.

Os LIFs VIP cobrem apenas a rede frontend/data.

Dependendo da sua versão do ONTAP, você deve configurar LIFs de peering BGP no nó SVM, não no sistema ou na SVM de dados. Em 9,8, os LIFs BGP são visíveis no cluster (sistema) SVM e os SVMs de nó não estão mais presentes.

Cada SVM de dados requer a configuração de todos os endereços potenciais de gateway de primeiro salto (normalmente, o endereço IP de peering do roteador BGP), de modo que o caminho de dados de retorno esteja disponível se ocorrer uma migração de LIF ou failover de MetroCluster.

As LIFs BGP são específicas de nós, semelhantes às LIFs entre clusters - cada nó tem uma configuração exclusiva, que não precisa ser replicado para os nós do local de DR.

A existência do v0a (v0b e assim por diante) valida continuamente a conetividade, garantindo que uma migração de LIF ou failover seja bem-sucedida (ao contrário do L2, onde uma configuração quebrada só é visível após a interrupção).

Uma grande diferença de arquitetura é que os clientes não devem mais compartilhar a mesma sub-rede IP que o VIP de SVMs de dados. Um roteador L3 com recursos apropriados de resiliência e redundância de nível empresarial habilitados (por exemplo, VRRP/HSRP) deve estar no caminho entre o armazenamento e os clientes para que o VIP funcione corretamente.

O processo de atualização confiável do BGP permite migrações de LIF mais suaves, pois elas são marginalmente mais rápidas e têm menor chance de interrupção para alguns clientes

Você pode configurar o BGP para detetar algumas classes de comportamentos incorretos de rede ou switch mais rápido do que o LACP, se configurado de acordo.

O BGP externo (EBGP) usa números diferentes entre nós ONTAP e roteadores de peering e é a implantação preferida para facilitar a agregação e redistribuição de rotas nos roteadores. O BGP interno (IBGP) e o uso de refletores de rota não são impossíveis, mas fora do escopo de uma configuração VIP direta.

Após a implantação, você deve verificar se o SVM de dados está acessível quando o LIF virtual associado é migrado entre todos os nós em cada local (incluindo switchover de MetroCluster) para verificar a configuração correta das rotas estáticas para o mesmo SVM de dados.

O VIP funciona para a maioria dos protocolos baseados em IP (NFS, SMB, iSCSI).

Configure os componentes de hardware do MetroCluster

Partes de uma configuração IP do MetroCluster

Ao Planejar sua configuração IP do MetroCluster, você deve entender os componentes de hardware e como eles se interconetam.

Principais elementos de hardware

Uma configuração IP do MetroCluster inclui os seguintes elementos-chave de hardware:

- Controladores de storage

  As controladoras de storage são configuradas como dois clusters de dois nós.

- Rede IP

  Esta rede IP back-end fornece conetividade para dois usos distintos:

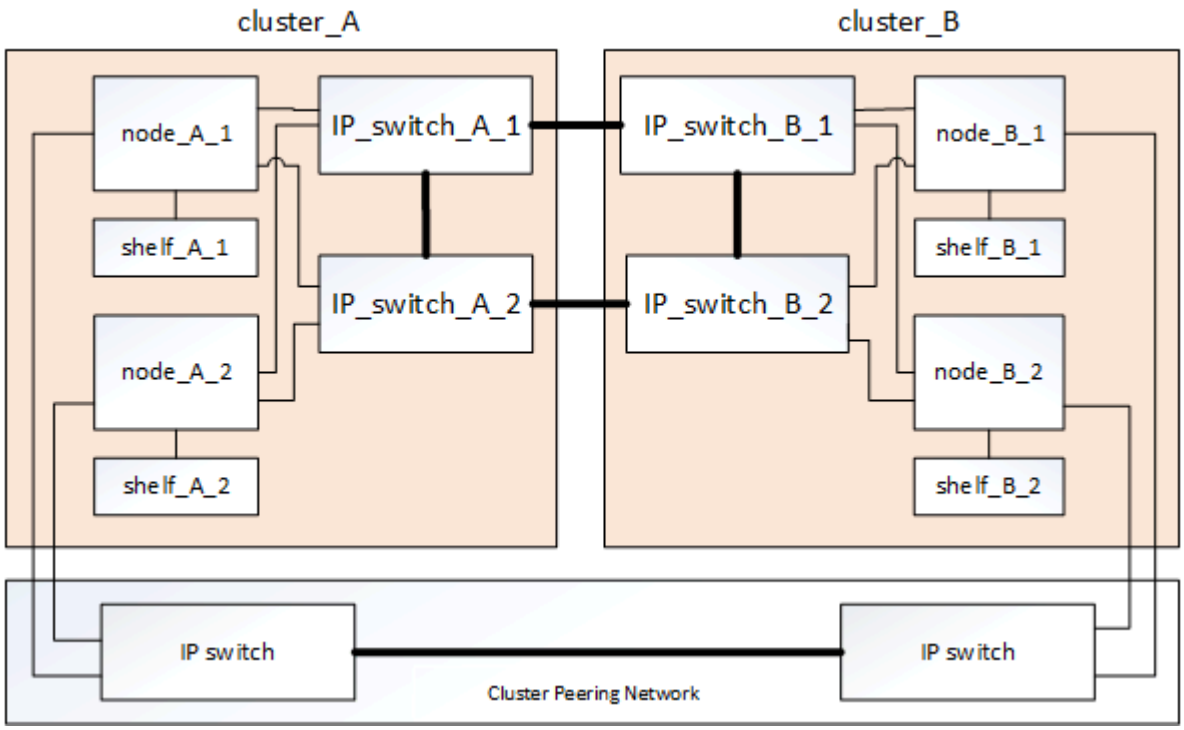
  - Conetividade de cluster padrão para comunicações intra-cluster.

    Essa é a mesma funcionalidade de switch de cluster usada em clusters ONTAP não comutados da MetroCluster.

  - Conectividade de back-end MetroCluster para replicação de dados de storage e cache não volátil.

- Rede de peering de cluster

  A rede de peering de cluster fornece conetividade para espelhamento da configuração do cluster, que inclui a configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.



Grupos de recuperação de desastres (DR)

Uma configuração IP do MetroCluster consiste em um grupo de DR de quatro nós.

A ilustração a seguir mostra a organização de nós em uma configuração de MetroCluster de quatro nós:

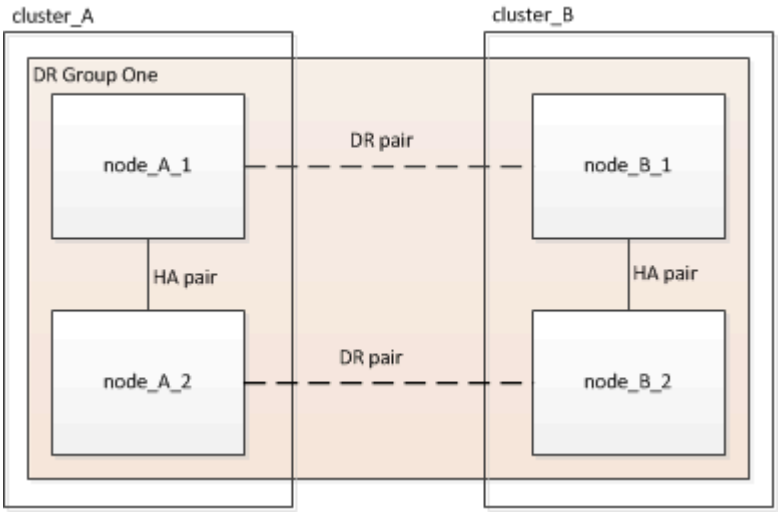
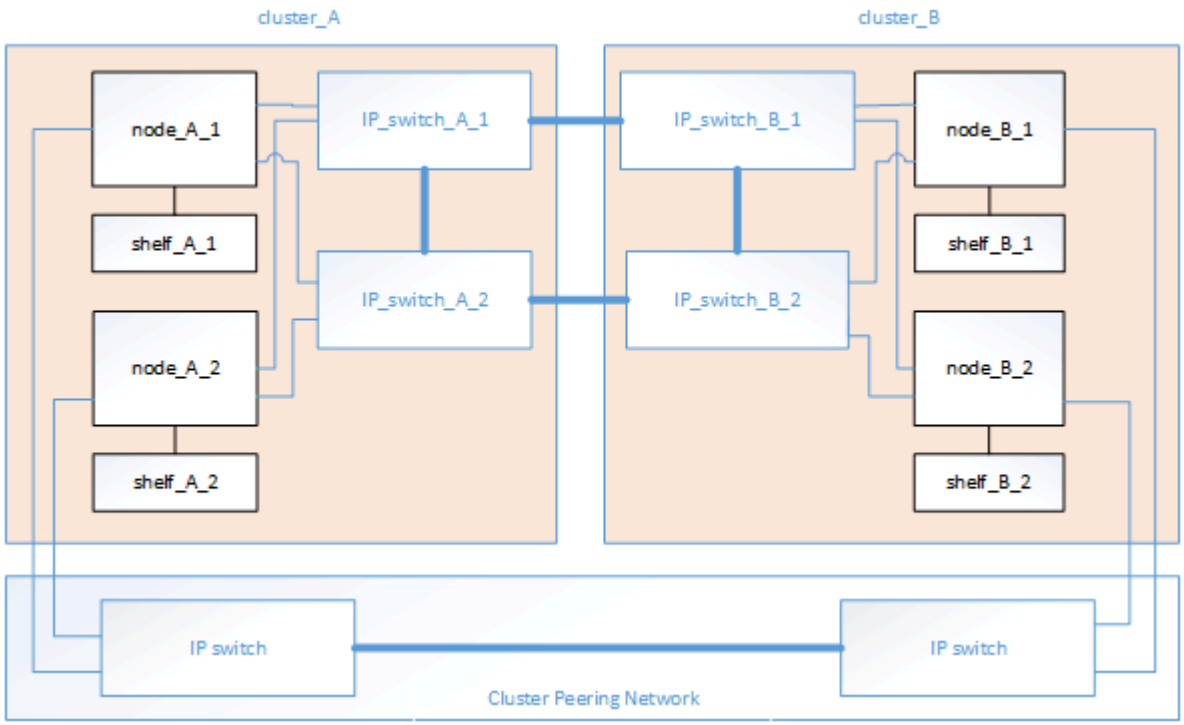


Ilustração dos pares de HA locais em uma configuração do MetroCluster

Cada local do MetroCluster consiste em controladores de storage configurados como um par de HA. Isso permite redundância local para que, se um controlador de storage falhar, seu parceiro de HA local possa assumir o controle. Essas falhas podem ser tratadas sem uma operação de switchover do MetroCluster.

As operações de failover de HA local e giveback são executadas com os comandos de failover de storage, da mesma maneira que uma configuração que não é MetroCluster.

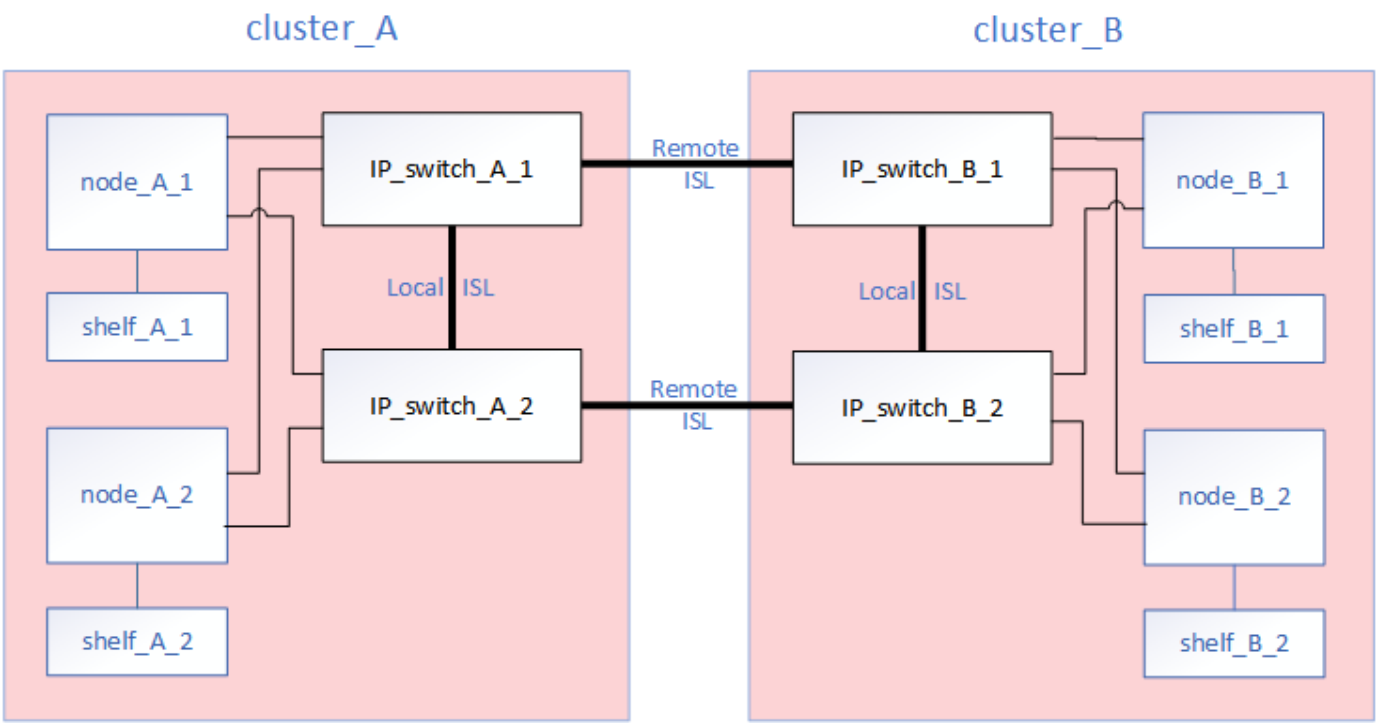


Informações relacionadas

"Conceitos de ONTAP"

Ilustração da rede de interligação de cluster e IP MetroCluster

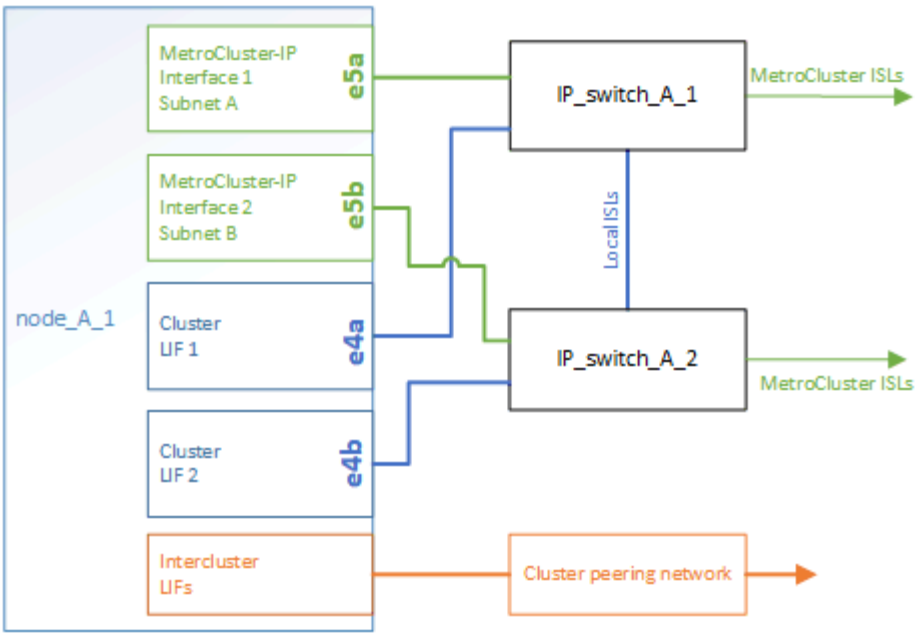
Os clusters do ONTAP geralmente incluem uma rede de interconexão de cluster para tráfego entre os nós no cluster. Nas configurações IP do MetroCluster, essa rede também é usada para transportar tráfego de replicação de dados entre os sites do MetroCluster.



Cada nó na configuração IP do MetroCluster tem interfaces dedicadas para conexão com a rede IP de back-end:

- Duas interfaces IP MetroCluster
- Duas interfaces de cluster locais

A ilustração a seguir mostra essas interfaces. O uso da porta mostrado é para um sistema AFF A700 ou FAS9000.



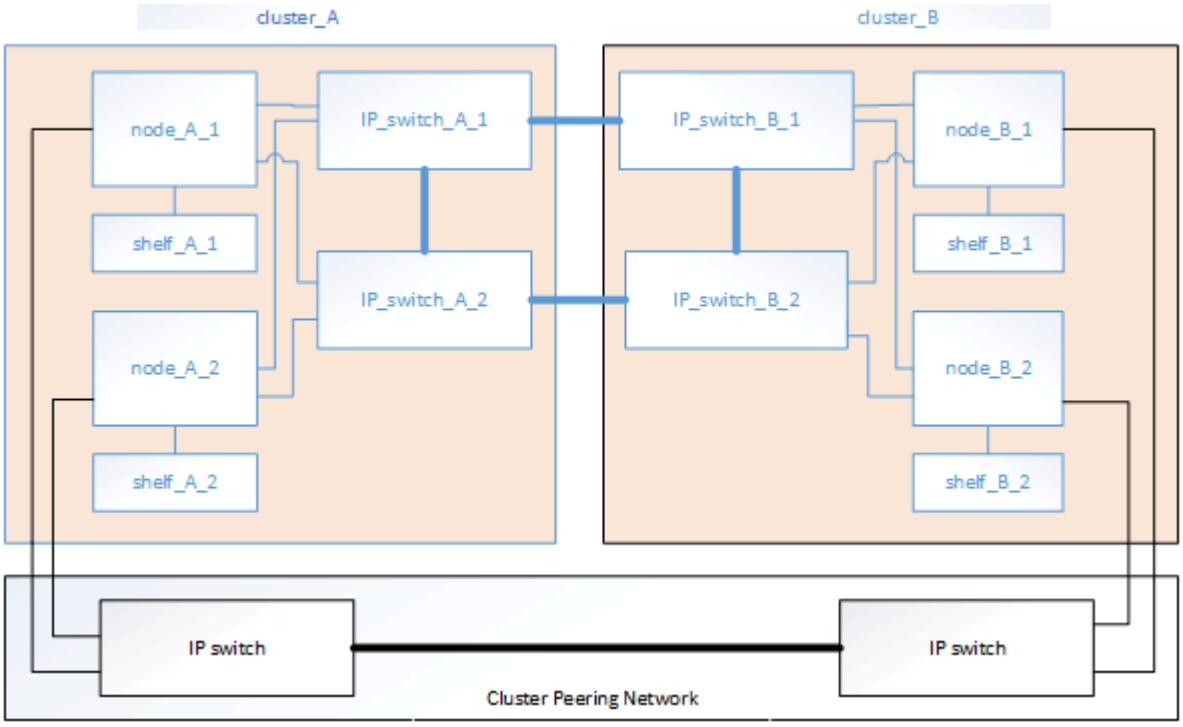
Informações relacionadas

"Considerações para configurações IP do MetroCluster"

Ilustração da rede de peering de cluster

Os dois clusters na configuração do MetroCluster são direcionados por meio de uma rede de peering de cluster fornecida pelo cliente. O peering de cluster suporta o espelhamento síncrono de máquinas virtuais de armazenamento (SVMs, anteriormente conhecido como VServers) entre os sites.

As LIFs entre clusters devem ser configuradas em cada nó na configuração do MetroCluster e os clusters devem ser configurados para peering. As portas com os LIFs entre clusters são conetadas à rede de peering de cluster fornecida pelo cliente. A replicação da configuração SVM é realizada por meio dessa rede por meio do Configuration Replication Service.



Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

"Considerações para configurar o peering de cluster"

"Cabeamento das conexões de peering de cluster"

"Peering dos clusters"

Componentes IP do MetroCluster necessários e convenções de nomenclatura

Ao Planejar sua configuração IP do MetroCluster, você deve entender os componentes de hardware e software necessários e suportados. Para conveniência e clareza, você também deve entender as convenções de nomenclatura usadas para componentes em exemplos ao longo da documentação.

Software e hardware suportados

O hardware e o software devem ser suportados para a configuração IP do MetroCluster.

"NetApp Hardware Universe"

Ao usar sistemas AFF, todos os módulos do controlador na configuração do MetroCluster devem ser configurados como sistemas AFF.

Requisitos de redundância de hardware em uma configuração IP MetroCluster

Devido à redundância de hardware na configuração IP do MetroCluster, há dois de cada componente em cada local. Os sites são arbitrariamente atribuídos às letras A e B, e os componentes individuais são arbitrariamente atribuídos os números 1 e 2.

Requisitos de cluster do ONTAP em uma configuração IP do MetroCluster

As configurações IP do MetroCluster exigem dois clusters ONTAP, um em cada local do MetroCluster.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Requisitos de switch IP em uma configuração IP MetroCluster

As configurações IP do MetroCluster requerem quatro switches IP. Os quatro switches formam duas malhas de armazenamento de switch que fornecem o ISL entre cada um dos clusters na configuração IP do MetroCluster.

Os switches IP também fornecem comunicação entre clusters entre os módulos do controlador em cada cluster.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
  - IP_switch_A_1
  - IP_switch_A_2
- Local B: Cluster_B
  - IP_switch_B_1
  - IP_switch_B_2

Requisitos do módulo do controlador em uma configuração IP do MetroCluster

As configurações IP do MetroCluster requerem quatro ou oito módulos de controlador.

Os módulos de controladora em cada local formam um par de HA. Cada módulo de controladora tem um parceiro de recuperação de desastres no outro local.

Cada módulo do controlador deve estar executando a mesma versão do ONTAP. Os modelos de plataforma compatíveis dependem da versão ONTAP:

- As novas instalações IP do MetroCluster em sistemas FAS não são suportadas no ONTAP 9.4.

  As configurações de IP MetroCluster existentes em sistemas FAS podem ser atualizadas para ONTAP 9.4.

- A partir do ONTAP 9.5, são suportadas novas instalações MetroCluster IP em sistemas FAS.
- A partir do ONTAP 9.4, os módulos de controlador configurados para ADP são suportados.

Nomes de exemplo

Os seguintes nomes de exemplo são usados na documentação:

- Local A: Cluster_A
  - controller_A_1
  - controller_A_2
- Local B: Cluster_B
  - controller_B_1
  - controller_B_2

Requisitos de adaptador Gigabit Ethernet em uma configuração IP MetroCluster

As configurações IP do MetroCluster usam um adaptador Ethernet de 40/100 Gbps ou 10/25 Gbps para as interfaces IP para os switches IP usados para a malha IP do MetroCluster.

As portas integradas são incorporadas ao hardware do controlador (slot 0) e não podem ser substituídas, portanto, o slot necessário para o adaptador não é aplicável.

Modelo de plataforma	Adaptador Gigabit Ethernet necessário	Ranhura necessária para o adaptador	Portas

AFF A900, ASA A900 e FAS9500	X91146A	Slot 5, slot 7	e5b, e7b
AFF A700 e FAS9000	X91146A-C	Ranhura 5	e5a, e5b
AFF A800, AFF C800, ASA A800 e ASA C800	Portas de X1146A GbE/integradas	Slot 1/não aplicável para portas integradas	e0b. e1b
FAS8300, AFF A400, ASA A400, ASA C400 e AFF C400	X1146A	Ranhura 1	e1a, e1b
AFF A300 e FAS8200	X1116A	Ranhura 1	e1a, e1b
FAS2750, AFF A150, ASA A150 e AFF A220	Portas integradas	Não aplicável	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250 e AFF C250	Portas integradas	Não aplicável	e0c, e0d
AFF A320	Portas integradas	Não aplicável	e0g, e0h
AFF A70	X50132A	Ranhura 2	e2a, e2b
AFF A90 e AFF A1K	X50132A	Slot 2, slot 3	e2b, e3b **Observação:** as portas E2A e E3A devem permanecer não utilizadas. O uso dessas portas para redes front-end ou peering não é suportado.

"Saiba mais sobre atribuição automática de unidades e sistemas ADP em configurações IP do MetroCluster".

Requisitos de pool e unidade (mínimo suportado)

São recomendadas oito gavetas de disco SAS (quatro gavetas em cada local) para permitir a propriedade de disco por compartimento.

Uma configuração IP MetroCluster de quatro nós requer a configuração mínima em cada local:

- Cada nó tem pelo menos um pool local e um pool remoto no local.
- Pelo menos sete unidades em cada pool.

  Em uma configuração de MetroCluster de quatro nós com um único agregado de dados espelhados por nó, a configuração mínima requer 24 discos no local.

Em uma configuração mínima suportada, cada pool tem o seguinte layout de unidade:

- Três unidades raiz
- Três unidades de dados
- Uma unidade sobressalente

Em uma configuração mínima com suporte, pelo menos um compartimento é necessário por local.

As configurações do MetroCluster são compatíveis com RAID-DP e RAID4.

Considerações sobre o local da unidade para compartimentos parcialmente preenchidos

Para a atribuição automática correta de unidades ao usar compartimentos com metade população (12 unidades em um compartimento de 24 unidades), as unidades devem estar localizadas nos slots 0-5 e 18-23.

Em uma configuração com um compartimento parcialmente preenchido, as unidades precisam ser distribuídas uniformemente nos quatro quadrantes da gaveta.

Considerações sobre o local da unidade para unidades internas AFF A800

Para a implementação correta do recurso ADP, os slots de disco do sistema AFF A800 devem ser divididos em trimestres e os discos devem ser localizados simetricamente nos trimestres.

Um sistema AFF A800 tem 48 compartimentos de unidade. As baías podem ser divididas em quartos:

- Quarto um:
  - Baías 0 - 5
  - Baías 24 - 29
- Quarto trimestre dois:
  - Baías 6 - 11
  - Baías 30 - 35
- Terceiro trimestre:
  - Baías 12 - 17
  - Baías 36 - 41
- Quarto trimestre:
  - Baías 18 - 23
  - Baías 42 - 47

Se este sistema estiver preenchido com 16 unidades, elas devem ser distribuídas simetricamente entre os quatro trimestres:

- Quatro unidades no primeiro trimestre: 0, 1, 2, 3
- Quatro unidades no segundo trimestre: 6, 7, 8, 9
- Quatro unidades no terceiro trimestre: 12, 13, 14, 15
- Quatro unidades no quarto trimestre: 18, 19, 20, 21

Misturando módulos IOM12 e IOM 6 em uma pilha

Sua versão do ONTAP deve suportar a mistura de prateleiras. Consulte a "Ferramenta de Matriz de interoperabilidade NetApp (IMT)" para ver se a sua versão do ONTAP suporta mistura de prateleiras.

Para obter mais detalhes sobre a mistura de prateleiras, consulte "Gavetas de adição dinâmica com IOM12 módulos para uma stack de gavetas com IOM6 módulos"

Colocar em pilha os componentes de hardware

Se você não recebeu o equipamento já instalado em armários, você deve colocar os componentes em rack.

Sobre esta tarefa

Esta tarefa tem de ser executada em ambos os sites da MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   O espaço em rack depende do modelo de plataforma dos módulos do controlador, dos tipos de switch e do número de pilhas de compartimento de disco na sua configuração.

2. Aterre-se corretamente.
3. Instale os módulos do controlador no rack ou gabinete.

   "Instruções de instalação e configuração dos sistemas AFF A220/FAS2700"

   "Instruções de instalação e configuração de sistemas AFF A250"

   "Instruções de instalação e configuração de sistemas AFF A300"

   "Sistemas AFF A320: Instalação e configuração"

   "Instruções de instalação e configuração de sistemas AFF A400"

   "Instruções de instalação e configuração de sistemas AFF A700"

   "Instruções de instalação e configuração de sistemas AFF A800"

   "Instruções de instalação e configuração de sistemas FAS500f"

   "Instruções de instalação e configuração de sistemas FAS8200"

   "Instruções de instalação e configuração dos sistemas FAS8300 e FAS8700"

   "Instruções de instalação e configuração de sistemas FAS9000"

4. Instale os switches IP no rack ou gabinete.
5. Instale as gavetas de disco, ligue-as e, em seguida, defina as IDs das gaveta.

   - É necessário desligar cada compartimento de disco.
   - IDs de gaveta exclusivas são altamente recomendadas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster para auxiliar na solução de problemas.

Não faça cabos com gavetas de disco destinadas a conter agregados sem espelhamento no momento. Você deve esperar para implantar gavetas destinadas a agregados sem espelhamento até que a configuração do MetroCluster esteja concluída e somente as implante depois de usar o `metrocluster modify -enable-unmirrored-aggr -deployment true` comando.

Cable os switches IP MetroCluster

Usando as tabelas de portas com a ferramenta RcfFileGenerator ou várias configurações do MetroCluster

Você deve entender como usar as informações nas tabelas de portas para gerar corretamente seus arquivos RCF.

Antes de começar

Reveja estas considerações antes de utilizar as tabelas:

- As tabelas a seguir mostram o uso da porta para o local A. o mesmo cabeamento é usado para o local B.
- Os switches não podem ser configurados com portas de velocidades diferentes (por exemplo, uma combinação de portas de 100 Gbps e portas de 40 Gbps).
- Mantenha o controle do grupo de portas MetroCluster (MetroCluster 1, MetroCluster 2, etc.). Você precisará dessas informações ao usar a ferramenta RcfFileGenerator, conforme descrito mais adiante neste procedimento de configuração.
- O "RcfFileGenerator para MetroCluster IP" também fornece uma visão geral do cabeamento por porta para cada switch. Use esta visão geral do cabeamento para verificar o cabeamento.

Cabeamento de configurações de MetroCluster de oito nós

Para a configuração do MetroCluster executando o ONTAP 9.8 e anterior, alguns procedimentos que são executados para fazer a transição de uma atualização exigem a adição de um segundo grupo de DR de quatro nós à configuração para criar uma configuração temporária de oito nós. A partir do ONTAP 9.9,1, são suportadas configurações permanentes de MetroCluster de oito nós.

Sobre esta tarefa

Para tais configurações, você usa o mesmo método descrito acima. Em vez de um segundo MetroCluster, você está fazendo o cabeamento de um grupo adicional de DR de quatro nós.

Por exemplo, sua configuração inclui o seguinte:

- Interrutores Cisco 3132Q-V.
- MetroCluster 1: Plataformas FAS2750
- MetroCluster 2: Plataformas AFF A700 (essas plataformas estão sendo adicionadas como um segundo grupo de DR de quatro nós)

Passos

1. Para o MetroCluster 1, faça o cabeamento dos switches Cisco 3132Q-V usando a tabela para a plataforma FAS2750 e as linhas para interfaces MetroCluster 1.
2. Para o MetroCluster 2 (o segundo grupo DR), faça o cabeamento dos switches Cisco 3132Q-V usando a tabela para a plataforma AFF A700 e as linhas para interfaces MetroCluster 2.

Atribuições de porta de plataforma para switches Cisco 3132Q-V.

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Reveja estas diretrizes antes de utilizar as tabelas:

- Se você configurar o switch para a transição MetroCluster FC para IP, a porta 5, a porta 6, a porta 13 ou a porta 14 podem ser usadas para conetar as interfaces de cluster locais do nó MetroCluster FC. Consulte "RcfFileGenerator"o e os arquivos de cabeamento gerados para obter mais detalhes sobre o cabeamento dessa configuração. Para todas as outras conexões, você pode usar as atribuições de uso de portas listadas nas tabelas.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é…	Use esta tabela de cabeamento…
FAS2750, AFF A220	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 1)
FAS9000, AFF A700	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 2)
AFF A800, ASA A800	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 3)

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 1)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS2750 ou AFF A220 para um switch Cisco 3132Q-V:

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS9000 ou AFF A700 para um switch Cisco 3132Q-V:

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema AFF A800 ou ASA A800 para um switch Cisco 3132Q-V:

Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Reveja estas considerações antes de utilizar as tabelas:

- As tabelas a seguir mostram o uso da porta para o local A. o mesmo cabeamento é usado para o local B.
- Os switches não podem ser configurados com portas de velocidades diferentes (por exemplo, uma combinação de portas de 100 Gbps e portas de 40 Gbps).
- Se você estiver configurando um único MetroCluster com os switches, use o grupo de portas **MetroCluster 1**.

  Mantenha o controle do grupo de portas MetroCluster (MetroCluster 1, MetroCluster 2, MetroCluster 3 ou MetroCluster 4). Você precisará dele ao usar a ferramenta RcfFileGenerator como descrito mais adiante neste procedimento de configuração.

- O RcfFileGenerator para MetroCluster IP também fornece uma visão geral de cabeamento por porta para cada switch.

Use esta visão geral do cabeamento para verificar o cabeamento.

- O arquivo RCF versão v2,10 ou posterior é necessário para o modo breakout 25G para ISLs MetroCluster.
- O ONTAP 9.13,1 ou posterior e o arquivo RCF versão 2,00 são necessários para usar uma plataforma diferente do FAS8200 ou do AFF A300 no grupo "MetroCluster 4".

> A versão do arquivo RCF é diferente da versão da ferramenta RCFfilegerator usada para gerar o arquivo. Por exemplo, você pode gerar um arquivo RCF versão 2,00 usando o RCFfilegerator v1,6c.

Cabeamento de duas configurações MetroCluster para os switches

Ao fazer o cabeamento de mais de uma configuração MetroCluster para um switch Cisco 3132Q-V, você deve fazer o cabeamento de cada MetroCluster de acordo com a tabela apropriada. Por exemplo, se estiver cabendo um FAS2750 e um AFF A700 ao mesmo switch Cisco 3132Q-V. Em seguida, você faz o cabo do FAS2750 de acordo com "MetroCluster 1" na Tabela 1, e do AFF A700 de acordo com "MetroCluster 2" ou "MetroCluster 3" na Tabela 2. Não é possível ligar fisicamente o FAS2750 e o AFF A700 como "MetroCluster 1".

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é…	Use esta tabela de cabeamento…
AFF A150, ASA A150, FAS2750, AFF A220 FAS500f, AFF C250, ASA C250, AFF A250, ASA A250	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 1)
FAS8200, AFF A300	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 2)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 3)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 4)
AFF A70 AFF A90 AFF A1K **Nota:** estes sistemas requerem o ONTAP 9.15,1 ou posterior.	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 5)

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 1)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch Cisco 3232C ou 9336C:

Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS8200 ou AFF A300 para um switch Cisco 3232C ou 9336C:

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, MetroCluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled	

Se você estiver atualizando a partir de arquivos RCF mais antigos, a configuração de cabeamento pode estar usando portas no grupo "MetroCluster 4" (portas 25/26 e 29/30).

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 3)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A320, FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 para um switch Cisco 3232C ou 9336C:

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

O uso de portas no grupo "MetroCluster 4" requer o ONTAP 9.13,1 ou posterior.

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 4)

Revise as atribuições de portas da plataforma para enviar um sistema FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 para um switch Cisco 3232C ou 9336C:

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

O uso de portas no grupo "MetroCluster 4" requer o ONTAP 9.13,1 ou posterior.

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C (grupo 5)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A70, AFF A90 ou AFF A1K para um switch Cisco 3232C ou 9336C:

Os sistemas nesta tabela requerem ONTAP 9.15,1 ou posterior.

Switch Port	Port use	AFF A70		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
2							
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
4							
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2b	e3b	e2b	e3b	e2b	e3b
10							
11	MetroCluster 2, MetroCluster interface	e2b	e3b	e2b	e3b	e2b	e3b
12							
13	MetroCluster 3, MetroCluster interface	e2b	e3b	e2b	e3b	e2b	e3b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2b	e3b	e2b	e3b	e2b	e3b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Atribuições de porta de plataforma para um switch compartilhado Cisco 9336C-FX2

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Reveja estas considerações antes de utilizar as tabelas:

- Pelo menos uma configuração do MetroCluster ou grupo de DR deve ser compatível com gavetas NS224 conectadas ao switch.
- As plataformas que não dão suporte a gavetas NS224 conectadas a switch só podem ser conectadas como uma segunda configuração MetroCluster ou como um segundo grupo de DR.
- O RcfFileGenerator só mostra as plataformas elegíveis quando a primeira plataforma é selecionada.
- A conexão de configurações de um MetroCluster de oito ou dois de quatro nós requer o ONTAP 9.14,1 ou posterior.

Escolha a tabela de cabeamento correta para sua configuração

Reveja a tabela de atribuições de portas correta para a sua configuração. Existem dois conjuntos de tabelas de cabeamento nesta seção:

- Tabelas de cabeamento para controladores que se conectam às gavetas NS224 conectadas ao switch
- Tabelas de cabeamento para controladores que não se conectam às gavetas NS224 conectadas ao switch

Controladoras conectadas às gavetas NS224 conectadas ao switch

Determine a tabela de atribuições de portas que você deve seguir para os controladores que se conetam às gavetas NS224 conectadas ao switch.

Plataforma	Use esta tabela de cabeamento…
AFF A320 AFF C400, ASA C400 AFF A400, ASA A400	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 1)
AFF A700 AFF C800, ASA C800, AFF A800 AFF A900, ASA A900	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 2)
AFF A90 AFF A70 AFF A1K **Nota:** estes sistemas requerem o ONTAP 9.15,1 ou posterior.	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 3)

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 1)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A320, AFF C400, ASA C400, AFF A400 ou ASA A400 que esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
18							
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b				
28		NSM-2, e0a	NSM-2, e0b				
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se

você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A700, AFF C800, ASA C800, AFF A800, AFF A900 ou ASA A900 que esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
18							
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A90, AFF A70 ou AFF A1K que esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Os sistemas nesta tabela requerem ONTAP 9.15,1 ou posterior.

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A70		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17 18	MetroCluster 1, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
19 20	MetroCluster 2, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2. e0a	NSM-2. e0b	NSM-2. e0a	NSM-2. e0b	NSM-2. e0a	NSM-2. e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Para um cluster conetado a switch, as portas de cluster idênticas nos nós AFF A90 ou AFF A70 devem estar no mesmo switch. Por exemplo, e1a em node1 e e1a em node2 devem ser conetados a um switch de cluster. Da mesma forma, a segunda porta de cluster de ambos os nós deve ser conetada ao segundo switch de cluster. A ligação cruzada de portas HA de cluster partilhado, onde e1a de node1 está ligada a IP_Switch_x_1 e e1a de node2 está ligada a IP_Switch_x_2, impede a falha de comunicação HA.

Controladores não se conectam às gavetas NS224 conectadas por switch

Determine a tabela de atribuições de portas que você deve seguir para os controladores que não estão se conetando às gavetas NS224 conectadas ao switch.

Plataforma	Use esta tabela de cabeamento…
AFF A150, ASA A150 FAS2750, AFF A220	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 4)

Plataforma	Use esta tabela de cabeamento…
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 5)
FAS8200, AFF A300	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 6)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 7)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 8)
AFF A70 AFF A90 AFF A1K **Nota:** estes sistemas requerem o ONTAP 9.15,1 ou posterior.	Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 9)

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 4)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A150, ASA A150, FAS2750 ou AFF A220 que não esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 5)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 que não esteja conetando as gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
9/2-4		disabled	
10/1		e0c	e0d
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
11/2-4		disabled	
12/1		e0c	e0d
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 6)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS8200 ou AFF A300 que não esteja conetando as gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 7)

Revise as atribuições de portas da plataforma para fazer cabo de um sistema AFF A320, FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 que não esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
3 4	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
5-6	Unused	disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
11 12	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17-36	Unused	disabled		disabled		disabled	

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 8)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS9000 Cisco, AFF A800 AFF A900, ASA A800 ASA A900, FAS9500, AFF A700 ou AFF C800 que não esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado ASA C800 9336C-FX2:

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
3 4	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
5-6	Unused	disabled		disabled		disabled	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
13 14 15 16	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17-36	Unused	disabled		disabled		disabled	

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de porta de plataforma de switch compartilhado Cisco 9336C-FX2 (grupo 9)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A70, AFF A90 ou AFF A1K que não esteja conetando gavetas NSS24 conetadas a switch a um switch compartilhado Cisco 9336C-FX2:

Os sistemas nesta tabela requerem ONTAP 9.15,1 ou posterior.

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	AFF A70		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
2							
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
10							
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Atribuições de portas de plataforma para switches IP BES-53248 com suporte da Broadcom

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Os switches não podem ser usados com portas ISL remotas de diferentes velocidades (por exemplo, uma porta de 25 Gbps conetada a uma porta ISL de 10 Gbps).

Revise essas informações antes de usar as tabelas:

- Se você configurar o switch para a transição MetroCluster FC para IP, as seguintes portas serão usadas dependendo da plataforma de destino escolhida:

Plataforma-alvo	Porta
Plataformas FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 ou FAS8700	Portas 1 - 6, 10Gbps
Plataformas FAS8200 ou AFF A300	Portas 3 - 4 e 9 - 12, 10Gbps

- Os sistemas AFF A320 configurados com switches BES-53248 Broadcom podem não suportar todos os recursos.

  Qualquer configuração ou recurso que exija que as conexões do cluster local estejam conetadas a um switch não é suportado. Por exemplo, as seguintes configurações e procedimentos não são suportados:

  - Configurações de MetroCluster de oito nós
  - Transição das configurações MetroCluster FC para MetroCluster IP
  - Atualizando uma configuração de IP MetroCluster de quatro nós (ONTAP 9.8 e posterior)

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é…	Use esta tabela de cabeamento…
AFF A150, ASA A150 FAS2750 AFF A220	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 1)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 2)
FAS8200, AFF A300	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 3)
AFF A320	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 4)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 5)

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 1)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A150, ASA A150, FAS2750 ou AFF A220 para um switch BES-53248 da Broadcom:

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused	disabled	
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Nota 1**: O uso dessas portas requer uma licença adicional.
- Se ambas as configurações do MetroCluster estiverem usando a mesma plataforma, a NetApp recomenda selecionar o grupo "MetroCluster 3" para uma configuração e o grupo "MetroCluster 4" para a outra configuração. Se as plataformas forem diferentes, você deve selecionar "MetroCluster 3" ou "MetroCluster 4" para a primeira configuração e "MetroCluster 1" ou "MetroCluster 2" para a segunda configuração.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Nota 1**: O uso dessas portas requer uma licença adicional.
- Se ambas as configurações do MetroCluster estiverem usando a mesma plataforma, a NetApp recomenda selecionar o grupo "MetroCluster 3" para uma configuração e o grupo "MetroCluster 4" para a outra configuração. Se as plataformas forem diferentes, você deve selecionar "MetroCluster 3" ou "MetroCluster 4" para a primeira configuração e "MetroCluster 1" ou "MetroCluster 2" para a segunda configuração.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS8200 ou AFF A300 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface Not used during Transition	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Nota 1**: O uso dessas portas requer uma licença adicional.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 4)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema AFF A320 para um switch BES-53248 Broadcom:

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
56			

- **Nota 1**: O uso dessas portas requer uma licença adicional.
- **Nota 2**: Apenas um único MetroCluster de quatro nós usando sistemas AFF A320 pode ser conetado ao switch.

Os recursos que exigem um cluster comutado não são suportados nesta configuração. Isso inclui os procedimentos de transição FC para IP do MetroCluster e atualização técnica.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 5)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 ou FAS8700 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see Note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

- **Nota 1**: O uso dessas portas requer uma licença adicional.
- **Nota 2**: Apenas um único MetroCluster de quatro nós usando sistemas AFF A320 pode ser conetado ao switch.

  Os recursos que exigem um cluster comutado não são suportados nesta configuração. Isso inclui os procedimentos de transição FC para IP do MetroCluster e atualização técnica.

Atribuições de porta de plataforma para switches IP SN2100 compatíveis com NVIDIA

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Configurações compatíveis

As seguintes configurações não são suportadas atualmente:

- Transição de MetroCluster FC para IP

Revise essas considerações antes de usar as tabelas de configuração

- A conexão de configurações de MetroCluster de oito ou dois nós requer o ONTAP 9.14,1 ou posterior e o arquivo RCF versão 2,00 ou posterior.

> A versão do arquivo RCF é diferente da versão da ferramenta RCFfilegerator usada para gerar o arquivo. Por exemplo, você pode gerar um arquivo RCF versão 2,00 usando o RCFfilegerator v1,6c.

- Se você fizer o cabo de várias configurações do MetroCluster, siga a respetiva tabela. Por exemplo:
  - Se você fizer o cabo de duas configurações MetroCluster de quatro nós do tipo AFF A700, conete o primeiro MetroCluster mostrado como "MetroCluster 1" e o segundo MetroCluster mostrado como "MetroCluster 2" na tabela AFF A700.

> As portas 13 e 14 podem ser usadas no modo de velocidade nativo que suporta 40 Gbps e 100 Gbps, ou no modo de breakout para suportar 4 x 25 Gbps ou 4 x 10 Gbps. Se eles usam o modo de velocidade nativa, eles são representados como portas 13 e 14. Se eles usam o modo breakout, 4 x 25 Gbps ou 4 x 10 Gbps, então eles são representados como portas 13s0-3 e 14s0-3.

As seções a seguir descrevem o contorno físico do cabeamento. Você também pode consultar o "RcfFileGenerator" para obter informações detalhadas sobre cabeamento.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é…	Use esta tabela de cabeamento…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 1)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700 FAS9000, AFF A700	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 2)
AFF C800, ASA C800 AFF A800, ASA A800 FAS9500 AFF A900, ASA A900	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 3)
AFF A70 AFF A90 AFF A1K **Nota:** estes sistemas requerem o ONTAP 9.15,1 ou posterior.	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 4)

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 1)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 2)

Revise as atribuições de portas da plataforma para enviar um sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000 ou AFF A700 para um switch NVIDIA SN2100:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a
2							
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a
4							
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a
6							
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
8							
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
10							
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 3)

Revise as atribuições de portas da plataforma para enviar um sistema AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Nota 1: Se estiver a utilizar um adaptador X91440A (40Gbps), utilize as portas e4a e e4e ou e4a e e8a. Se você estiver usando um adaptador X91153A (100Gbps), use as portas e4a e e4b ou e4a e e8a.

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 4)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A90, AFF A70 ou AFF A1K para um switch NVIDIA SN2100:

Os sistemas nesta tabela requerem ONTAP 9.15,1 ou posterior.

Switch Port	Port use	AFF A70		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
2							
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
4							
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a
6							
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2b	e3b	e2b	e3b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

Cabeamento das portas de peering, dados e gerenciamento da controladora

Você deve fazer o cabeamento das portas do módulo do controlador usadas para peering de cluster, gerenciamento e conetividade de dados.

Esta tarefa deve ser executada em cada módulo do controlador na configuração do MetroCluster.

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

   O peering de cluster pode ser feito em portas dedicadas ou em portas de dados. O uso de portas dedicadas fornece maior taxa de transferência para o tráfego de peering de cluster.

   "Configuração expressa de peering de cluster e SVM"

2. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

   Use as instruções de instalação da sua plataforma no "Documentação dos sistemas de hardware da ONTAP".

   > Os sistemas IP da MetroCluster não têm portas de alta disponibilidade (HA) dedicadas. Dependendo da sua plataforma, o tráfego de HA é servido usando o MetroCluster, o cluster local ou a interface de cluster/MetroCluster compartilhado. Ao usar *Documentação de sistemas de hardware ONTAP* para instalar sua plataforma, você não deve seguir as instruções para fazer o cabeamento do cluster e das portas HA.

Configure os switches IP MetroCluster

Configuração de switches IP Broadcom

Você deve configurar os switches IP Broadcom para uso como interconexão de cluster e para conetividade IP MetroCluster de back-end.

> A sua configuração requer licenças adicionais (6 licença de porta de 100 GB) nos seguintes cenários:

- Você usa as portas 53 e 54 como um ISL MetroCluster de 40 Gbps ou 100 Gbps.
- Você usa uma plataforma que coneta o cluster local e as interfaces MetroCluster às portas 49 - 52.

Redefinindo o switch IP Broadcom para os padrões de fábrica

Antes de instalar uma nova versão do software do switch e RCFs, você deve apagar as configurações do switch Broadcom e executar a configuração básica.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Mude para o prompt de comando elevado (`#`): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Apague a configuração de inicialização e remova o banner

   a. Apagar a configuração de arranque:

      `erase startup-config`

      ```
      (IP_switch_A_1) #erase startup-config

      Are you sure you want to clear the configuration? (y/n) y

      (IP_switch_A_1) #
      ```

      Este comando não apaga o banner.

   b. Remova o banner:

      `no set clibanner`

   ```
   (IP_switch_A_1) #configure
   (IP_switch_A_1)(Config) # no set clibanner
   (IP_switch_A_1)(Config) #
   ```

3. Reinicie o switch: **`(IP_switch_A_1) #reload`**

   ```
   Are you sure you would like to reset the system? (y/n) y
   ```

   Se o sistema perguntar se deseja salvar a configuração não salva ou alterada antes de recarregar o switch, selecione **não**.

4. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   O usuário padrão é "'admin'", e nenhuma senha é definida. É apresentado um aviso semelhante ao seguinte:

   ```
   (Routing)>
   ```

5. Mude para o prompt de comando elevado:

   `enable`

   ```
   Routing)> enable
   (Routing) #
   ```

6. Defina o protocolo da porta de serviço como `none`:

   `serviceport protocol none`

   ```
   (Routing) #serviceport protocol none
   Changing protocol mode will reset ip configuration.
   Are you sure you want to continue? (y/n) y

   (Routing) #
   ```

7. Atribua o endereço IP à porta de serviço:

   `serviceport ip` *`ip-address netmask gateway`*

   O exemplo a seguir mostra um endereço IP atribuído à porta de serviço "10.10.10.10" com a sub-rede "255.255.255.0" e o gateway "10.10.10.1":

   ```
   (Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
   ```

8. Verifique se a porta de serviço está configurada corretamente:

   `show serviceport`

   O exemplo a seguir mostra que a porta está ativa e os endereços corretos foram atribuídos:

   ```
   (Routing) #show serviceport

   Interface Status.............................. Up
   IP Address..................................... 10.10.10.10
   Subnet Mask.................................... 255.255.255.0
   Default Gateway................................ 10.10.10.1
   IPv6 Administrative Mode....................... Enabled
   IPv6 Prefix is ................................
   fe80::dac4:97ff:fe56:87d7/64
   IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
   Configured IPv4 Protocol....................... None
   Configured IPv6 Protocol....................... None
   IPv6 AutoConfig Mode........................... Disabled
   Burned In MAC Address.......................... D8:C4:97:56:87:D7

   (Routing) #
   ```

9. Se desejar, configure o servidor SSH.

O arquivo RCF desativa o protocolo Telnet. Se você não configurar o servidor SSH, você só poderá acessar a ponte usando a conexão de porta serial.

a. Gerar chaves RSA.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. Gerar chaves DSA (opcional)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Se você estiver usando a versão compatível com FIPS do EFOS, gere as chaves ECDSA. O exemplo a seguir cria as teclas com um comprimento de 521. Os valores válidos são 256, 384 ou 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Ative o servidor SSH.

Se necessário, saia do contexto de configuração.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

Se as chaves já existem, então você pode ser solicitado a sobrescrevê-las.

10. Se desejar, configure o domínio e o servidor de nomes:

`configure`

O exemplo a seguir mostra `ip domain` os comandos e `ip name server`:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Se desejar, configure o fuso horário e a sincronização de horário (SNTP).

O exemplo a seguir mostra os `sntp` comandos, especificando o endereço IP do servidor SNTP e o fuso horário relativo.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

Para o EFOS versão 3.10.0.3 e posterior, use o `ntp` comando, como mostrado no exemplo a seguir:

```
> (Config)# ntp ?

authenticate             Enables NTP authentication.
authentication-key       Configure NTP authentication key.
broadcast                Enables NTP broadcast mode.
broadcastdelay           Configure NTP broadcast delay in microseconds.
server                   Configure NTP server.
source-interface         Configure the NTP source-interface.
trusted-key              Configure NTP authentication key number for
trusted time source.
vrf                      Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Configure o nome do switch:

    `hostname IP_switch_A_1`

    O prompt do switch exibirá o novo nome:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Guardar a configuração:

    `write memory`

Você recebe prompts e saída semelhantes ao seguinte exemplo:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Download e instalação do software Broadcom switch EFOS

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa deve ser repetida em cada switch na configuração IP do MetroCluster.

Observe o seguinte:

- Ao atualizar do EFOS 3,4.x.x para o EFOS 3,7.x.x ou posterior, o switch deve estar executando o EFOS 3.4.4.6 (ou versão 3,4.x.x posterior). Se você estiver executando uma versão antes disso, atualize o switch para EFOS 3.4.4.6 (ou versão posterior 3,4.x.x) primeiro, então atualize o switch para EFOS 3,7.x.x ou posterior.
- A configuração para o EFOS 3,4.x.x e 3,7.x.x ou posterior é diferente. Alterar a versão do EFOS de 3,4.x.x para 3,7.x.x ou posterior, ou vice-versa, requer que o switch seja redefinido para os padrões de fábrica e os arquivos RCF para que a versão do EFOS correspondente seja (re)aplicada. Este procedimento requer acesso através da porta do console serial.
- A partir da versão 3,7.x.x do EFOS ou posterior, uma versão não compatível com FIPS e compatível com FIPS está disponível. Diferentes etapas se aplicam ao passar de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa. Alterar o EFOS de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa redefinirá o switch para os padrões de fábrica. Este procedimento requer acesso através da porta do console serial.

Passos

1. Transfira o firmware do switch a partir do "Site de suporte da Broadcom".
2. Verifique se sua versão do EFOS é compatível com FIPS ou não compatível com FIPS usando o `show fips status` comando. Nos exemplos a seguir `IP_switch_A_1`, está usando EFOS compatível com FIPS e `IP_switch_A_2` está usando EFOS não compatível com FIPS.

Exemplo 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Exemplo 2

```
IP_switch_A_2 #show fips status
                      ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

3. Use a tabela a seguir para determinar qual método você deve seguir:

Procedimento	Versão atual do EFOS	Nova versão EFOS	Passos de alto nível
Etapas para atualizar o EFOS entre duas versões (não) compatíveis com FIPS	3.4.x.x	3.4.x.x	Instale a nova imagem EFOS utilizando o método 1) as informações de configuração e licença são mantidas
3.4.4.6 (ou posterior 3,4.x.x)	3,7.x.x ou posterior não compatível com FIPS	Atualize o EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3,7.x.x ou posterior	3,7.x.x ou posterior não compatível com FIPS
3.4.4.6 (ou posterior 3,4.x.x)	Downgrade EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3,4.x.x	3,7.x.x ou posterior não compatível com FIPS	
Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas	3,7.x.x ou posterior compatível com FIPS	3,7.x.x ou posterior compatível com FIPS	Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas

Passos para atualizar para/a partir de uma versão EFOS compatível com FIPS	Não compatível com FIPS	Compatível com FIPS	Instalação da imagem EFOS usando o método 2. A configuração do switch e as informações da licença serão perdidas.

- Método 1: Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup
- Método 2: Etapas para atualizar o EFOS usando a instalação do ONIE os

Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup

Só pode executar as seguintes etapas se ambas as versões do EFOS forem não compatíveis com FIPS ou ambas as versões do EFOS forem compatíveis com FIPS.

Não utilize estes passos se uma versão for compatível com FIPS e a outra não for compatível com FIPS.

Passos

1. Copie o software do interrutor para o interrutor: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   Neste exemplo, o arquivo do sistema operacional efos-3,4.4,6.stk é copiado do servidor SFTP em 50.50.50.50 para a partição de backup. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename........................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Configure o switch para inicializar a partir da partição de backup na próxima reinicialização do switch:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Verifique se a nova imagem de inicialização estará ativa na próxima inicialização:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Guardar a configuração:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Reinicie o switch:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Aguarde até que o switch seja reiniciado.

Em cenários raros, o switch pode falhar ao inicializar. Siga o Etapas para atualizar o EFOS usando a instalação do ONIE os para instalar a nova imagem.

7. Se alterar a mudança de EFOS 3,4.x.x para EFOS 3,7.x.x ou vice-versa, siga os dois procedimentos a seguir para aplicar a configuração correta (RCF):
   a. Redefinindo o switch IP Broadcom para os padrões de fábrica
   b. Download e instalação dos arquivos RCF Broadcom
8. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Etapas para atualizar o EFOS usando a instalação do ONIE os

Pode executar as seguintes etapas se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS. Estas etapas podem ser usadas para instalar a imagem EFOS 3,7.x.x não compatível com FIPS do ONIE se o switch não inicializar.

Passos

1. Inicialize o switch no modo de instalação ONIE.

   Durante a inicialização, selecione ONIE quando a seguinte tela for exibida:

```
+----------------------------------------------------------------------+
|EFOS                                                                  |
|*ONIE                                                                 |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
|                                                                      |
+----------------------------------------------------------------------+
```

   Depois de selecionar "ONIE", o switch irá então carregar e apresentar-lhe as seguintes opções:

```
+--------------------------------------------------------------------+
|*ONIE: Install OS                                                   |
| ONIE: Rescue                                                       |
| ONIE: Uninstall OS                                                 |
| ONIE: Update ONIE                                                  |
| ONIE: Embed ONIE                                                   |
| DIAG: Diagnostic Mode                                              |
| DIAG: Burn-In Mode                                                 |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
+--------------------------------------------------------------------+
```

O switch agora será inicializado no modo de instalação ONIE.

2. Pare a descoberta ONIE e configure a interface ethernet

   Quando a seguinte mensagem for exibida, pressione <enter> para chamar o console ONIE:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   A descoberta ONIE continuará e as mensagens serão impressas no console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configure a interface ethernet e adicione a rota utilizando `ifconfig eth0 <ipAddress> netmask <netmask> up` e. `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Verifique se o servidor que hospeda o arquivo de instalação ONIE está acessível:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Instale o novo software do interrutor

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

O software irá instalar e, em seguida, reiniciar o interrutor. Deixe o switch reiniciar normalmente para a nova versão do EFOS.

6. Verifique se o novo software do switch está instalado

`show bootvar`

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Conclua a instalação

   O switch reiniciará sem nenhuma configuração aplicada e redefinirá os padrões de fábrica. Siga os dois procedimentos para configurar as configurações básicas do switch e aplicar o arquivo RCF conforme descrito nos dois documentos a seguir:

   a. Configure as definições básicas do interrutor. Siga o passo 4 e posterior: Redefinindo o switch IP Broadcom para os padrões de fábrica
   b. Crie e aplique o arquivo RCF conforme descrito em Download e instalação dos arquivos RCF Broadcom

Download e instalação dos arquivos RCF Broadcom

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Sobre esta tarefa

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Existem quatro arquivos RCF, um para cada um dos quatro switches na configuração IP do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro RCF
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt

Os arquivos RCF para EFOS versão 3.4.4.6 ou posterior versão 3,4.x.x. e EFOS versão 3.7.0.4 são diferentes. Você precisa ter certeza de que criou os arquivos RCF corretos para a versão EFOS em que o switch está sendo executado.

Versão de EFOS	Versão do ficheiro RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Passos

1. Gere os arquivos RCF Broadcom para MetroCluster IP.
   a. Transfira o. "RcfFileGenerator para MetroCluster IP"
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:

   a. Copie os arquivos RCF para o primeiro switch:
   `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

   Neste exemplo, o arquivo RCF "BES-53248_v1,32_Switch-A1.txt" é copiado do servidor SFTP em "50.50.50.50" para o flash de inicialização local. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /RcfFiles/
Filename..................................... BES-
53248_v1.32_Switch-A1.txt
Data Type.................................... Config Script
Destination Filename......................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"************************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Verifique se o arquivo RCF está salvo como um script:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Aplicar o script RCF:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"************************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Guardar a configuração:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Reinicie o switch:

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

a. Repita os passos anteriores para cada uma das outras três centrais, certificando-se de copiar o ficheiro RCF correspondente para o comutador correspondente.

3. Recarregue o interrutor:

```
reload
```

```
IP_switch_A_1# reload
```

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:

> Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

Para detalhes da porta ISL

Executar o comando `show port all`.

Para obter detalhes do canal da porta

Executar o comando `show port-channel all`.

2. Desative as portas ISL e os canais de portas não utilizados.

   Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Configurar switches IP Cisco

Configurar switches IP Cisco

Você deve configurar os switches IP Cisco para uso como interconexão de cluster e para conetividade IP do MetroCluster de back-end.

Sobre esta tarefa

Vários dos procedimentos nesta seção são procedimentos independentes e você só precisa executar aqueles para os quais você é direcionado ou é relevante para a sua tarefa.

Repor as predefinições de fábrica do interrutor IP do Cisco

Antes de instalar qualquer arquivo RCF, você deve apagar a configuração do switch Cisco e executar a configuração básica. Este procedimento é necessário quando você deseja reinstalar o mesmo arquivo RCF depois de uma instalação anterior falhar, ou se você quiser instalar uma nova versão de um arquivo RCF.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Repor as predefinições de fábrica do interrutor:

   a. Apagar a configuração existente:

      `write erase`

b. Recarregue o software do switch:

```
reload
```

O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt "'Cancelar provisionamento automático e continuar com a configuração normal? (sim/não)", `you should respond `yes` para continuar.

c. No assistente de configuração, introduza as definições básicas do interrutor:

- Palavra-passe de administrador
- Mudar nome
- Configuração de gerenciamento fora da banda
- Gateway predefinido
- Serviço SSH (RSA)

Depois de concluir o assistente de configuração, o switch reinicia.

d. Quando solicitado, introduza o nome de utilizador e a palavra-passe para iniciar sessão no comutador.

O exemplo a seguir mostra os prompts e as respostas do sistema ao configurar o switch. Os colchetes de ângulo (<<<) mostram onde você insere as informações.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Você insere informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e seleciona SSH com RSA.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

O conjunto final de prompts completa a configuração:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Guardar a configuração:

```
IP_switch-A-1# copy running-config startup-config
```

3. Reinicie o switch e aguarde até que o switch recarregue:

```
IP_switch-A-1# reload
```

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Transferir e instalar o software Cisco switch NX-os

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Passos

1. Transfira o ficheiro de software NX-os suportado.

   "Transferência do software Cisco"

2. Copie o software do interrutor para o interrutor:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   Neste exemplo, o arquivo nxos.7.0.3.I4.6.bin é copiado do servidor SFTP 10.10.99.99 para o flash de inicialização local:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verifique em cada switch se os arquivos NX-os estão presentes no diretório bootflash de cada switch:

   ```
   dir bootflash:
   ```

   O exemplo a seguir mostra que os arquivos estão presentes no IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Instale o software do interrutor:

   `install all nxos bootflash:nxos.version-number.bin`

   O interrutor recarregará (reiniciará) automaticamente após a instalação do software do interrutor.

   O exemplo a seguir mostra a instalação do software em IP_switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos               7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   Depois que o switch reiniciar, o prompt de login é exibido:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verifique se o software do switch foi instalado
`show version`

   O exemplo a seguir mostra a saída:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Transferir e instalar os ficheiros Cisco IP RCF

Você deve gerar e instalar o arquivo RCF em cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os

arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Existem quatro arquivos RCF, um para cada um dos quatro switches na configuração IP do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Passos

1. Gerar os arquivos RCF do Cisco para MetroCluster IP.
   a. Transfira o. "RcfFileGenerator para MetroCluster IP"
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

      As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:
   a. Copie os arquivos RCF para o primeiro switch:

      ```
      copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
      bootflash: vrf management
      ```

      Neste exemplo, o arquivo RCF NX3232_v1.80_Switch-A1.txt é copiado do servidor SFTP em 10.10.99.99 para o flash de inicialização local. Você deve usar o endereço IP do servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Repita a subetapa anterior para cada uma das outras três centrais, certificando-se de copiar o arquivo RCF correspondente para a central correspondente.

3. Verifique em cada switch se o arquivo RCF está presente no diretório bootflash de cada switch:

   `dir bootflash:`

   O exemplo a seguir mostra que os arquivos estão presentes no IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                   .
                   .
                   .
5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                   .
                   .
                   .

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Configure as regiões TCAM nos switches Cisco 3132Q-V e Cisco 3232C.

   Ignore esta etapa se você não tiver switches Cisco 3132Q-V ou Cisco 3232C.

   a. No interrutor Cisco 3132Q-V, defina as seguintes regiões TCAM:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. No switch Cisco 3232C, defina as seguintes regiões TCAM:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Depois de definir as regiões TCAM, salve a configuração e recarregue o switch:

```
copy running-config startup-config
reload
```

5. Copie o arquivo RCF correspondente do flash de inicialização local para a configuração em execução em cada switch:

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Copie os arquivos RCF da configuração em execução para a configuração de inicialização em cada switch:

   `copy running-config startup-config`

   Você deve ver saída semelhante ao seguinte:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Recarregue o interrutor:

   `reload`

```
IP_switch_A_1# reload
```

8. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Definição de correção de erro de avanço para sistemas que utilizam conetividade de 25 Gbps

Se o sistema estiver configurado usando conetividade de 25 Gbps, você precisará definir manualmente o parâmetro Correção de erros de Avanço (fec) para Desativado após a aplicação do arquivo RCF. O ficheiro RCF não aplica esta definição.

Sobre esta tarefa

As portas de 25 Gbps devem ser cabeadas antes de executar este procedimento.

"Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C"

Esta tarefa aplica-se apenas a plataformas que utilizam conetividade de 25 Gbps:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Esta tarefa deve ser executada em todos os quatro switches na configuração IP do MetroCluster.

Passos

1. Defina o parâmetro fec como Desligado em cada porta de 25 Gbps conetada a um módulo de controladora e copie a configuração em execução para a configuração de inicialização:

   a. Entre no modo de configuração: `config t`

   b. Especifique a interface de 25 Gbps para configurar: `interface interface-ID`

   c. Defina fec para Off (Desligado): `fec off`

   d. Repita as etapas anteriores para cada porta de 25 Gbps no switch.

   e. Sair do modo de configuração: `exit`

   O exemplo a seguir mostra os comandos da interface Ethernet1/25/1 no switch IP_switch_A_1:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Repita a etapa anterior nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identificar as portas ISL e os canais de portas não utilizados:

```
show interface brief
```

2. Desative as portas ISL e os canais de portas não utilizados.

   Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configure a criptografia MACsec em switches Cisco 9336C

A criptografia MACsec só pode ser aplicada às portas ISL WAN.

Configure a criptografia MACsec em switches Cisco 9336C

Você só deve configurar a criptografia MACsec nas portas ISL WAN executadas entre os sites. Você deve configurar o MACsec depois de aplicar o arquivo RCF correto.

Requisitos de licenciamento para MACsec

MACsec requer uma licença de segurança. Para obter uma explicação completa do esquema de licenciamento do Cisco NX-os e como obter e solicitar licenças, consulte a. "Guia de licenciamento do Cisco NX-os"

Habilite ISLs WAN de criptografia MACsec Cisco em configurações IP MetroCluster

Você pode ativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Ativar MACsec e MKA no dispositivo:

```
feature macsec
```

```
IP_switch_A_1(config)# feature macsec
```

3. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configure uma cadeia de chaves e chaves MACsec

Você pode criar uma cadeia de chaves MACsec ou chaves em sua configuração.

Key Lifetime e Hitless Key Rollover

Um chaveiro MACsec pode ter várias chaves pré-compartilhadas (PSKs), cada uma configurada com um ID de chave e uma vida útil opcional. Uma vida útil da chave especifica a hora em que a chave ativa e expira. Na ausência de uma configuração vitalícia, o tempo de vida padrão é ilimitado. Quando uma vida útil é configurada, o MKA passa para a próxima chave pré-compartilhada configurada no chaveiro após a expiração da vida útil. O fuso horário da chave pode ser local ou UTC. O fuso horário padrão é UTC. Uma chave pode rolar para uma segunda chave dentro do mesmo chaveiro se você configurar a segunda chave (no chaveiro) e configurar uma vida útil para a primeira chave. Quando o tempo de vida da primeira tecla expira, ela passa automaticamente para a próxima chave na lista. Se a mesma chave for configurada em ambos os lados do link ao mesmo tempo, a rolagem da chave será sem hitless (ou seja, a chave rolará sem interrupção de tráfego).

Passos

1. Entre no modo de configuração global:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Para ocultar a cadeia de carateres octeto de chave criptografada, substitua a cadeia por um caractere curinga na saída `show running-config` dos comandos e `show startup-config`:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

> A cadeia de carateres octeto também é oculta quando você salva a configuração em um arquivo.

   Por padrão, as chaves PSK são exibidas em formato criptografado e podem ser facilmente descriptografadas. Este comando aplica-se apenas às cadeias de chaves MACsec.

3. Crie uma cadeia de chaves MACsec para manter um conjunto de chaves MACsec e entrar no modo de configuração da cadeia de chaves MACsec:

`key chain name macsec`

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

4. Crie uma chave MACsec e entre no modo de configuração da chave MACsec:

   `key key-id`

   O intervalo é de 1 a 32 carateres de chave de dígitos hexadecimais e o tamanho máximo é de 64 carateres.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configure a cadeia de carateres octeto para a chave:

   `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```

   O argumento octet-string pode conter até 64 carateres hexadecimais. A chave octeto é codificada internamente, portanto a chave em texto claro não aparece na saída do `show running-config macsec` comando.

6. Configure uma vida útil de envio para a chave (em segundos):

   `send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

   Por padrão, o dispositivo trata a hora de início como UTC. O argumento de hora de início é a hora do dia e a data em que a chave se torna ativa. O argumento duração é o comprimento do tempo de vida em segundos. A duração máxima é de 2147483646 segundos (aproximadamente 68 anos).

7. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Exibe a configuração do keychain:

   `show key chain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configurar uma política MACsec

Passos

1. Entre no modo de configuração global:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Criar uma política MACsec:

   `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Configure uma das seguintes cifras, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256:

   `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configure a prioridade do servidor de chaves para quebrar o vínculo entre pares durante uma troca de chaves:

   `key-server-priority number`

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configure a política de segurança para definir o processamento de dados e pacotes de controle:

   `security-policy security policy`

   Escolha uma política de segurança das seguintes opções:

   - Must-Secure — os pacotes que não transportam cabeçalhos MACsec são descartados

- Should-secure - pacotes que não transportam cabeçalhos MACsec são permitidos (este é o valor padrão)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configure a janela de proteção de repetição para que a interface protegida não aceite um pacote que seja menor do que o tamanho da janela configurado: `window-size number`

   O tamanho da janela de proteção de repetição representa o máximo de quadros fora de sequência que o MACsec aceita e não são descartados. O intervalo é de 0 a 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configure o tempo em segundos para forçar um SAK rechavear:

   `sak-expiry-time time`

   Você pode usar este comando para alterar a chave da sessão para um intervalo de tempo previsível. A predefinição é 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configure uma das seguintes compensações de confidencialidade no quadro da camada 2 onde a criptografia começa:

   `conf-offsetconfidentiality offset`

   Escolha entre as seguintes opções:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

   Esse comando pode ser necessário para que os switches intermediários usem cabeçalhos de pacotes (dmac, smac, etype) como tags MPLS.

9. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Apresentar a configuração da política MACsec:

    `show macsec policy`

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Ative a criptografia Cisco MACsec nas interfaces

1. Entre no modo de configuração global:

    `configure terminal`

    ```
    IP_switch_A_1# configure terminal
    IP_switch_A_1(config)#
    ```

2. Selecione a interface que você configurou com criptografia MACsec.

    Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

    ```
    IP_switch_A_1(config)# interface ethernet 1/15
    switch(config-if)#
    ```

3. Adicione o chaveiro e a política a serem configurados na interface para adicionar a configuração MACsec:

    `macsec keychain keychain-name policy policy-name`

    ```
    IP_switch_A_1(config-if)# macsec keychain 1 policy abc
    ```

4. Repita as etapas 1 e 2 em todas as interfaces onde a criptografia MACsec deve ser configurada.
5. Copie a configuração em execução para a configuração de inicialização:

    `copy running-config startup-config`

    ```
    IP_switch_A_1(config)# copy running-config startup-config
    ```

Desative os ISLs de WAN de criptografia Cisco MACsec em configurações IP do MetroCluster

Talvez seja necessário desativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

`configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Desative a configuração MACsec no dispositivo:

`macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Selecionar a opção "não" restaura o recurso MACsec.

3. Selecione a interface que você já configurou com o MACsec.

Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remova o chaveiro e a política configurados na interface para remover a configuração MACsec:

`no macsec keychain keychain-name policy policy-name`

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

5. Repita as etapas 3 e 4 em todas as interfaces onde o MACsec está configurado.
6. Copie a configuração em execução para a configuração de inicialização:

`copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Verificando a configuração do MACsec

Passos

1. Repita **All** dos procedimentos anteriores no segundo switch dentro da configuração para estabelecer uma sessão MACsec.
2. Execute os seguintes comandos para verificar se ambos os switches estão criptografados com êxito:

a. Executar: `show macsec mka summary`

b. Executar: `show macsec mka session`

c. Executar: `show macsec mka statistics`

Você pode verificar a configuração do MACsec usando os seguintes comandos:

Comando	Exibe informações sobre…
`show macsec mka session interface typeslot/port number`	A sessão MACsec MKA para uma interface específica ou para todas as interfaces
`show key chain name`	A configuração da cadeia de chaves
`show macsec mka summary`	A configuração MACsec MKA
`show macsec policy policy-name`	A configuração para uma política MACsec específica ou para todas as políticas MACsec

Configure o switch NVIDIA IP SN2100

Você deve configurar os switches IP NVIDIA SN2100 para uso como interconexão de cluster e para conetividade IP MetroCluster de back-end.

Reponha o switch NVIDIA IP SN2100 para os padrões de fábrica

Você pode escolher entre os seguintes métodos para redefinir um switch para as configurações padrão de fábrica.

- Reponha o interrutor utilizando a opção de ficheiro RCF
- Baixe e instale o software Cumulus

Reponha o switch usando a opção de arquivo RCF

Antes de instalar uma nova configuração RCF, você deve reverter as configurações do switch NVIDIA.

Sobre esta tarefa

Para restaurar o switch para as configurações padrão, execute o arquivo RCF com a `restoreDefaults` opção. Esta opção copia os ficheiros de cópia de segurança originais para a sua localização original e, em seguida, reinicia o interrutor. Após a reinicialização, o switch fica online com a configuração original que existia quando você executou o arquivo RCF pela primeira vez para configurar o switch.

Os seguintes detalhes de configuração não são redefinidos:

- Configuração de usuário e credencial
- Configuração da porta de rede de gerenciamento, eth0

Todas as outras alterações de configuração que ocorrem durante a aplicação do ficheiro RCF são revertidas para a configuração original.

Antes de começar

- Tem de configurar o interrutor de acordo Baixe e instale o arquivo NVIDIA RCFcom . Se não tiver

configurado desta forma ou tiver configurado funcionalidades adicionais antes de executar o ficheiro RCF, não pode utilizar este procedimento.

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch com uma conexão de console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Verifique se a configuração do RCF foi aplicada com sucesso com a mesma ou uma versão de arquivo RCF compatível e se os arquivos de backup existem.

A saída pode mostrar arquivos de backup, arquivos preservados ou ambos. Se arquivos de backup ou arquivos preservados não aparecerem na saída, você não poderá usar este procedimento.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Execute o arquivo RCF com a opção para restaurar os padrões: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Responda "sim" ao prompt. O interrutor reverte para a configuração original e reinicializa.
4. Aguarde até que o switch seja reiniciado.

   O switch é redefinido e mantém a configuração inicial, como configuração de rede de gerenciamento e credenciais atuais, conforme existiam antes de aplicar o arquivo RCF. Após a reinicialização, você pode aplicar uma nova configuração usando a mesma ou uma versão diferente do arquivo RCF.

Baixe e instale o software Cumulus

Sobre esta tarefa

Siga estas etapas se você quiser redefinir completamente o switch aplicando a imagem Cumulus.

Antes de começar

- Você deve estar conetado ao switch com uma conexão de console serial.
- A imagem do software Cumulus switch é acessível através de HTTP.

> Para obter mais informações sobre a instalação do Cumulus Linux, consulte "Visão geral da instalação e configuração dos switches NVIDIA SN2100"

- Você deve ter a senha raiz para `sudo` acesso aos comandos.

Passos

1. A partir do download do console Cumulus e coloque em fila a instalação do software do switch com o comando `onie-install -a -i` seguido do caminho do arquivo para o software do switch:

   Neste exemplo, o arquivo de firmware `cumulus-linux-4.4.3-mlx-amd64.bin` é copiado do servidor HTTP '50.50.50.50' para o switch local.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
##################################################################
# 100.0%
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
```

```
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
```

```
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Responda `y` ao aviso para confirmar a instalação quando a imagem é transferida e verificada.
3. Reinicie o switch para instalar o novo software: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> O interrutor reinicia e entra na instalação do software do interrutor, o que demora algum tempo. Quando a instalação estiver concluída, o interrutor reinicializa e permanece no prompt de 'login'.

4. Configure as definições básicas do interrutor
   a. Quando o switch é inicializado e no prompt de login, faça login e altere a senha.

> O nome de usuário é 'Cumulus' e a senha padrão é 'Cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configure a interface de rede de gerenciamento.

   Os comandos que você usa dependem da versão do firmware do switch que você está executando.

   > Os comandos de exemplo a seguir configuram o nome do host como IP_switch_A_1, o endereço IP como 10.10.10.10, a máscara de rede como 255.255.255.0 (24) e o endereço de gateway como 10.10.10.1.

Cumulus 4,4.x

Os comandos de exemplo a seguir configuram o nome do host, endereço IP, máscara de rede e gateway em um switch executando Cumulus 4,4.x.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

Cumulus 5,4.x e posterior

Os comandos de exemplo a seguir configuram o nome de host, endereço IP, máscara de rede e gateway em um switch executando Cumulus 5,4.x. ou posterior.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. Reinicie o switch usando o `sudo reboot` comando.

```
cumulus@cumulus:~$ sudo reboot
```

Quando o switch for reinicializado, você poderá aplicar uma nova configuração usando as etapas em Baixe e instale o arquivo NVIDIA RCF.

Baixe e instale os arquivos RCF do NVIDIA

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

- Você deve ter a senha raiz para `sudo` acesso aos comandos.
- O software do switch está instalado e a rede de gerenciamento está configurada.
- Você seguiu os passos para instalar inicialmente o switch usando o método 1 ou o método 2.
- Você não aplicou nenhuma configuração adicional após a instalação inicial.

> Se efetuar uma configuração adicional depois de reiniciar o comutador e antes de aplicar o ficheiro RCF, não poderá utilizar este procedimento.

Sobre esta tarefa

Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster (nova instalação) ou no comutador de substituição (substituição do comutador).

Passos

1. Gerar os arquivos RCF do NVIDIA para MetroCluster IP.
   a. Faça download do "RcfFileGenerator para MetroCluster IP".
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.
   c. Navegue para o seu diretório inicial. Se você estiver logado como 'Cumulus', o caminho do arquivo é `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

d. Transfira o ficheiro RCF para este diretório. O exemplo a seguir mostra que você usa SCP para baixar o arquivo `SN2100_v2.0.0_IP_switch_A_1.txt` do servidor '50.50.50.50' para o diretório principal e salvá-lo como `SN2100_v2.0.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
**********************************************************************
**
Banner of the SCP server
**********************************************************************
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Execute o arquivo RCF. O arquivo RCF requer uma opção para aplicar uma ou mais etapas. A menos que instruído pelo suporte técnico, execute o arquivo RCF sem a opção de linha de comando. Para verificar o estado de conclusão dos vários passos do ficheiro RCF, utilize a opção '-1' ou 'All' para aplicar todos os passos (pendentes).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

3. Se a sua configuração utilizar cabos DAC, ative a opção DAC nas portas do switch:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

O exemplo a seguir ativa a opção DAC para a porta `swp7`:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.00
    Running command: Enabling the DacOption for port swp7
    runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. Reinicie o switch depois de ativar a opção DAC nas portas do switch:

```
sudo reboot
```

> Ao definir a opção DAC para várias portas de switch, você só precisa reiniciar o switch uma vez.

Defina a velocidade da porta do switch para as interfaces IP do MetroCluster

Sobre esta tarefa

Use este procedimento para definir a velocidade da porta do switch para 100g para os seguintes sistemas:

- AFF A70
- AFF A90
- AFF A1K

Passo

1. Utilize o ficheiro RCF com a `runCmd` opção para definir a velocidade. Isso aplica a configuração e salva a configuração.

   Os comandos a seguir definem a velocidade para as interfaces MetroCluster `swp7` e `swp8`:

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
   ```

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
   ```

   Exemplo

   ```
   cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
   swp7 speed 100
   [sudo] password for cumulus: <password>
       Running cumulus version  : 5.4.0
       Running RCF file version : v2.20
       Running command: Setting switchport swp7 to 100G speed
       runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
       runCmd: 'nv set interface swp7 link speed 100G', ret: 0
       runCmd: committed, ret: 0
       Completion: SUCCESS
   cumulus@Switch-A-1:mgmt:~$
   ```

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:

   > Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

   ```
   net show interface
   ```

2. Desative as portas ISL e os canais de portas não utilizados usando o arquivo RCF.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

O seguinte comando de exemplo desativa a porta "swp14":

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Repita esta etapa para cada porta ou canal de porta não utilizado identificado.

Configurar switches IP MetroCluster para monitoramento de integridade

Nas configurações IP do MetroCluster, você pode configurar o SNMPv3 para monitorar a integridade dos switches IP.

Passo 1: Configure o usuário SNMPv3 em switches IP MetroCluster

Siga as etapas a seguir para configurar o usuário SNMPv3 nos switches IP do MetroCluster.

> Você deve usar os protocolos de autenticação e privacidade nos comandos. O uso de autenticação sem privacidade não é suportado.

Para switches IP Broadcom

Passos

1. Se o grupo de utilizadores 'network-admin' ainda não existir, crie-o:

```
(IP_switch_1) (Config)# snmp-server group network-admin v3 auth read
"Default"
```

2. Confirme se o grupo 'network-admin' foi criado:

```
(IP_switch_1) (Config)# show snmp group
```

3. Configure o usuário SNMPv3 em switches IP Broadcom:

```
(IP_switch_1)# config
(IP_switch_1) (Config)# snmp-server user <user_name> network-admin
[auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]
"<priv_password>"
```

Você deve usar aspas em torno das senhas de autenticação e privacidade, como mostrado no exemplo a seguir:

```
snmp-server user admin1 network-admin auth-md5 "password" priv-des
"password"
```

Para switches IP Cisco

Passos

1. Execute os seguintes comandos para configurar o usuário SNMPv3 em um switch IP Cisco:

```
IP_switch_A_1 # configure terminal
IP_switch_A_1 (config) # snmp-server user <user_name>  auth
[md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
```

2. Verifique se o usuário SNMPv3 está configurado no switch:

```
IP_switch_A_1(config) # show snmp user <user_name>
```

A saída de exemplo a seguir mostra que o usuário `admin` está configurado para SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User                 Auth      Priv(enforce) Groups
acl_filter

____                 ____      _____________ ______
__________

admin                md5       aes-128(no)   network-admin
```

Passo 2: Configure o usuário SNMPv3 no ONTAP

Siga as etapas a seguir para configurar o usuário SNMPv3 no ONTAP.

1. Configure o usuário SNMPv3 no ONTAP:

   ```
   security login create -user-or-group-name <user_name> -application snmp
   -authentication-method usm -remote-switch-ipaddress <ip_address>
   ```

2. Configure a monitorização do estado do comutador para monitorizar o comutador utilizando o novo utilizador SNMPv3:

   ```
   system switch ethernet modify -device <device_id> -snmp-version SNMPv3
   -community-or-username <user_name>
   ```

3. Verifique se o número de série do dispositivo que será monitorado com o usuário SNMPv3 recém-criado está correto:
   a. Apresentar o período de tempo de polling da monitorização do estado do interrutor:

      ```
      system switch ethernet polling-interval show
      ```

   b. Execute o seguinte comando após o período de tempo de polling ter decorrido:

      ```
      system switch ethernet show-all -instance -device <device_serial_number>
      ```

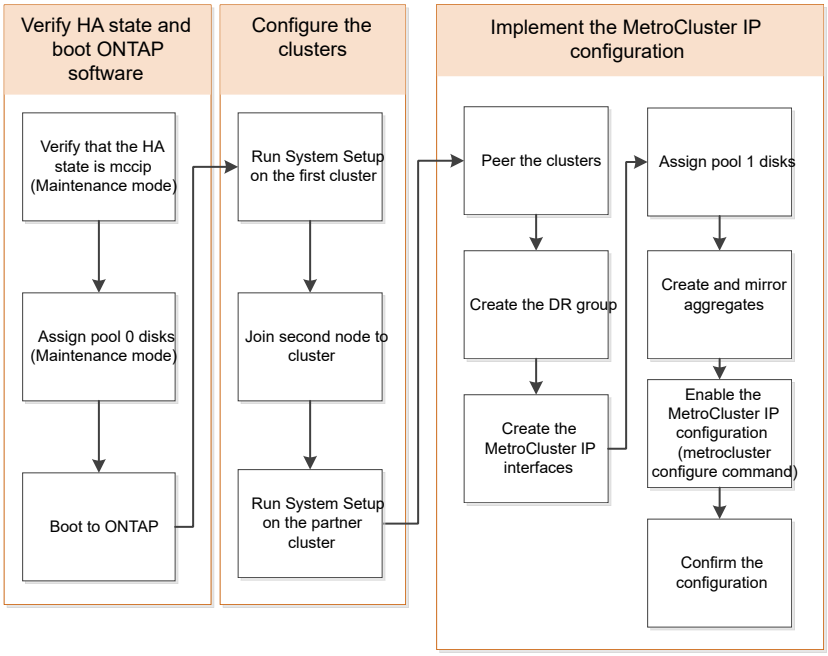
Configure o software MetroCluster no ONTAP

Configure o software MetroCluster usando a CLI

Configurando o software MetroCluster no ONTAP

É necessário configurar cada nó na configuração do MetroCluster no ONTAP, incluindo as configurações no nível do nó e a configuração dos nós em dois locais. Você também deve implementar a relação MetroCluster entre os dois sites.

Se um módulo do controlador falhar durante a configuração, "Cenários de falha do módulo do controlador durante a instalação do MetroCluster"consulte a .



Manipulação de configurações de oito nós

Uma configuração de oito nós consistirá em dois grupos de DR. Configure o primeiro grupo de DR usando as tarefas desta seção.

Em seguida, execute as tarefas em "Expansão de uma configuração IP MetroCluster de quatro nós para uma configuração de oito nós"

Recolha de informações necessárias

Você precisa reunir os endereços IP necessários para os módulos do controlador antes de iniciar o processo de configuração.

Você pode usar esses links para baixar arquivos csv e preencher as tabelas com informações específicas do seu site.

"Folha de cálculo de configuração IP do MetroCluster, site_A"

"Folha de cálculo de configuração IP do MetroCluster, site_B"

Semelhanças e diferenças entre configurações padrão de cluster e MetroCluster

A configuração dos nós em cada cluster em uma configuração MetroCluster é semelhante à dos nós em um cluster padrão.

A configuração do MetroCluster é baseada em dois clusters padrão. Fisicamente, a configuração deve ser simétrica, com cada nó tendo a mesma configuração de hardware e todos os componentes do MetroCluster devem ser cabeados e configurados. No entanto, a configuração básica de software para nós em uma configuração MetroCluster é a mesma para nós em um cluster padrão.

Etapa de configuração	Configuração padrão de cluster	Configuração do MetroCluster

Configurar LIFs de gerenciamento, cluster e dados em cada nó.	O mesmo em ambos os tipos de clusters	
Configure o agregado raiz.	O mesmo em ambos os tipos de clusters	
Configure o cluster em um nó no cluster.	O mesmo em ambos os tipos de clusters	
Junte o outro nó ao cluster.	O mesmo em ambos os tipos de clusters	
Crie um agregado de raiz espelhado.	Opcional	Obrigatório
Espreite os clusters.	Opcional	Obrigatório
Ative a configuração do MetroCluster.	Não se aplica	Obrigatório

Verificando o estado ha-config dos componentes

Em uma configuração IP do MetroCluster, você deve verificar se o estado ha-config dos componentes do controlador e do chassi está definido como "mccip" para que eles iniciem corretamente. Embora esse valor deva ser pré-configurado em sistemas recebidos de fábrica, você ainda deve verificar a configuração antes de continuar.

Se o estado HA do módulo do controlador e do chassis estiver incorreto, não poderá configurar o MetroCluster sem reiniciar o nó. Deve corrigir a definição utilizando este procedimento e, em seguida, inicializar o sistema utilizando um dos seguintes procedimentos:

- Em uma configuração IP do MetroCluster, siga as etapas em "Restaure os padrões do sistema em um módulo do controlador".
- Em uma configuração MetroCluster FC, siga as etapas em "Restaure os padrões do sistema e configurando o tipo HBA em um módulo do controlador".

Antes de começar

Verifique se o sistema está no modo Manutenção.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   ```
   ha-config show
   ```

   O estado de HA correto depende da configuração do MetroCluster.

Tipo de configuração MetroCluster	Estado HA para todos os componentes…

Configuração de FC MetroCluster de oito ou quatro nós	mcc
Configuração de FC MetroCluster de dois nós	mcc-2n
Configuração IP MetroCluster de oito ou quatro nós	mccip

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA correto para a sua configuração no módulo do controlador:

Tipo de configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify controller mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify controller mcc-2n`
Configuração IP MetroCluster de oito ou quatro nós	`ha-config modify controller mccip`

3. Se o estado do sistema apresentado do chassis não estiver correto, defina o estado HA correto para a sua configuração no chassis:

Tipo de configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify chassis mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify chassis mcc-2n`
Configuração IP MetroCluster de oito ou quatro nós	`ha-config modify chassis mccip`

4. Inicialize o nó no ONTAP:

   `boot_ontap`

5. Repita todo esse procedimento para verificar o estado de HA em cada nó na configuração do MetroCluster.

Restaurar padrões do sistema em um módulo do controlador

Redefinir e restaurar padrões nos módulos do controlador.

1. No prompt Loader, retorne variáveis ambientais à configuração padrão: `set-defaults`
2. Inicialize o nó no menu de inicialização: `boot_ontap menu`

   Depois de executar este comando, aguarde até que o menu de inicialização seja exibido.

3. Limpe a configuração do nó:

   - Se você estiver usando sistemas configurados para ADP, selecione a opção `9a` no menu de inicialização e responda `no` quando solicitado.

     Este processo é disruptivo.

     A tela a seguir mostra o prompt do menu de inicialização:

```
Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a
...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

   - Se o sistema não estiver configurado para ADP, digite `wipeconfig` no prompt do menu de inicialização e pressione Enter.

     A tela a seguir mostra o prompt do menu de inicialização:

```
Please choose one of the following:

    (1) Normal Boot.
    (2) Boot without /etc/rc.
    (3) Change password.
    (4) Clean configuration and initialize all disks.
    (5) Maintenance mode boot.
    (6) Update flash from backup config.
    (7) Install new software first.
    (8) Reboot node.
    (9) Configure Advanced Drive Partitioning.
    Selection (1-9)?  wipeconfig
This option deletes critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken over.
Are you sure you want to continue?: yes
Rebooting to finish wipeconfig request.
```

Atribuindo manualmente unidades ao pool 0

Se você não recebeu os sistemas pré-configurados de fábrica, talvez seja necessário atribuir manualmente as unidades do pool 0. Dependendo do modelo da plataforma e se o sistema está usando ADP, você deve atribuir manualmente unidades ao pool 0 para cada nó na configuração IP do MetroCluster. O procedimento utilizado depende da versão do ONTAP que está a utilizar.

Atribuição manual de unidades para o pool 0 (ONTAP 9.4 e posterior)

Se o sistema não tiver sido pré-configurado de fábrica e não atender aos requisitos de atribuição automática de unidades, você deverá atribuir manualmente as unidades 0 do pool.

Sobre esta tarefa

Este procedimento aplica-se às configurações que executam o ONTAP 9.4 ou posterior.

Para determinar se o sistema necessita de atribuição manual de disco, deve rever "Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior"o .

Execute estas etapas no modo Manutenção. O procedimento deve ser executado em cada nó na configuração.

Os exemplos nesta seção são baseados nas seguintes suposições:

- Unidades próprias Node_A_1 e node_A_2 em:
  - Site_A-shelf_1 (local)
  - Local_B-shelf_2 (remoto)
- Unidades próprias do nó_B_1 e do nó_B_2 em:

- Site_B-shelf_1 (local)
- Local_A-shelf_2 (remoto)

Passos

1. Apresentar o menu de arranque:

   `boot_ontap menu`

2. Selecione a opção 9a e responda `no` quando solicitado.

   A tela a seguir mostra o prompt do menu de inicialização:

```
Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a

...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

3. Quando o nó for reiniciado, pressione Ctrl-C quando solicitado a exibir o menu de inicialização e selecione a opção para **Inicialização do modo de manutenção**.

4. No modo Manutenção, atribua manualmente unidades para os agregados locais no nó:

   `disk assign *disk-id* -p 0 -s *local-node-sysid*`

   As unidades devem ser atribuídas simetricamente, de modo que cada nó tenha um número igual de unidades. As etapas a seguir referem-se a uma configuração com duas gavetas de storage em cada local.

   a. Ao configurar node_A_1, atribua manualmente unidades do slot 0 a 11 a pool0 do nó A1 a partir do site_A-shelf_1.
   b. Ao configurar node_A_2, atribua manualmente unidades do slot 12 a 23 a pool0 do nó A2 a partir do site_A-shelf_1.
   c. Ao configurar node_B_1, atribua manualmente unidades do slot 0 a 11 a pool0 do nó B1 a partir do site_B-shelf_1.
   d. Ao configurar node_B_2, atribua manualmente unidades do slot 12 a 23 a pool0 do nó B2 a partir do site_B-shelf_1.

5. Sair do modo de manutenção:

   `halt`

6. Apresentar o menu de arranque:

   `boot_ontap menu`

7. Repita estas etapas nos outros nós na configuração IP do MetroCluster.
8. Selecione a opção **4** no menu de inicialização em ambos os nós e deixe o sistema inicializar.
9. Prossiga para "Configurar o ONTAP".

Atribuição manual de unidades para o pool 0 (ONTAP 9.3)

Se você tiver pelo menos duas gavetas de disco para cada nó, use a funcionalidade de atribuição automática do ONTAP para atribuir automaticamente os discos locais (pool 0).

Sobre esta tarefa

Enquanto o nó estiver no modo Manutenção, primeiro é necessário atribuir um único disco nas prateleiras apropriadas ao pool 0. Em seguida, o ONTAP atribui automaticamente o restante dos discos na gaveta ao mesmo pool. Esta tarefa não é necessária nos sistemas recebidos de fábrica, que têm o pool 0 para conter o agregado raiz pré-configurado.

Este procedimento aplica-se às configurações que executam o ONTAP 9.3.

Este procedimento não é necessário se tiver recebido a configuração do MetroCluster de fábrica. Os nós da fábrica são configurados com pool 0 discos e agregados de raiz.

Esse procedimento só pode ser usado se você tiver pelo menos duas gavetas de disco para cada nó, o que permite a atribuição automática de discos no nível de compartimento. Se não for possível usar a atribuição automática no nível de compartimento, você deverá atribuir manualmente os discos locais para que cada nó tenha um pool local de discos (pool 0).

Estes passos têm de ser executados no modo de manutenção.

Os exemplos nesta seção assumem os seguintes compartimentos de disco:

- Node_A_1 possui discos em:
  - Site_A-shelf_1 (local)
  - Local_B-shelf_2 (remoto)
- O nó_A_2 está ligado a:
  - Site_A-shelf_3 (local)
  - Local_B-shelf_4 (remoto)
- O nó_B_1 está ligado a:
  - Site_B-shelf_1 (local)
  - Local_A-shelf_2 (remoto)
- O nó_B_2 está ligado a:
  - Site_B-shelf_3 (local)
  - Local_A-shelf_4 (remoto)

Passos

1. Atribua manualmente um único disco para agregado de raiz em cada nó:

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   A atribuição manual desses discos permite que o recurso de atribuição automática do ONTAP atribua o restante dos discos em cada compartimento.

   a. No node_A_1, atribua manualmente um disco do local site_A-shelf_1 ao pool 0.
   b. No node_A_2, atribua manualmente um disco do local site_A-shelf_3 ao pool 0.
   c. No node_B_1, atribua manualmente um disco do local site_B-shelf_1 ao pool 0.
   d. No node_B_2, atribua manualmente um disco do local site_B-shelf_3 ao pool 0.
2. Inicialize cada nó no local A, usando a opção 4 no menu de inicialização:

   Você deve concluir esta etapa em um nó antes de prosseguir para o próximo nó.

   a. Sair do modo de manutenção:

      `halt`

   b. Apresentar o menu de arranque:

      `boot_ontap menu`

   c. Selecione a opção 4 no menu de inicialização e prossiga.
3. Inicialize cada nó no local B, usando a opção 4 no menu de inicialização:

   Você deve concluir esta etapa em um nó antes de prosseguir para o próximo nó.

   a. Sair do modo de manutenção:

      `halt`

   b. Apresentar o menu de arranque:

```
boot_ontap menu
```

c. Selecione a opção 4 no menu de inicialização e prossiga.

Configurar o ONTAP

Depois de inicializar cada nó, você será solicitado a executar a configuração básica do nó e do cluster. Depois de configurar o cluster, você retorna à CLI do ONTAP para criar agregados e criar a configuração do MetroCluster.

Antes de começar

- Você deve ter cabeado a configuração do MetroCluster.

Se for necessário inicializar via rede os novos controladores, "Netboot os novos módulos do controlador"consulte .

Sobre esta tarefa

Essa tarefa deve ser executada em ambos os clusters na configuração do MetroCluster.

Passos

1. Ligue cada nó no site local se você ainda não o fez e deixe todos iniciarem completamente.

   Se o sistema estiver no modo Manutenção, você precisará emitir o comando halt para sair do modo Manutenção e, em seguida, emitir o `boot_ontap` comando para inicializar o sistema e chegar à configuração do cluster.

2. No primeiro nó em cada cluster, prossiga pelos prompts para configurar o cluster.

   a. Ative a ferramenta AutoSupport seguindo as instruções fornecidas pelo sistema.

      A saída deve ser semelhante ao seguinte:

```
Welcome to the cluster setup wizard.

    You can enter the following commands at any time:
    "help" or "?" - if you want to have a question clarified,
    "back" - if you want to change previously answered questions, and
    "exit" or "quit" - if you want to quit the cluster setup wizard.
    Any changes you made before quitting will be saved.

    You can return to cluster setup at any time by typing "cluster
setup".
    To accept a default or omit a question, do not enter a value.

    This system will send event messages and periodic reports to
NetApp Technical
    Support. To disable this feature, enter
    autosupport modify -support disable
    within 24 hours.

    Enabling AutoSupport can significantly speed problem
determination and
    resolution should a problem occur on your system.
    For further information on AutoSupport, see:
    http://support.netapp.com/autosupport/

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

b. Configure a interface de gerenciamento de nós respondendo aos prompts.

   Os prompts são semelhantes aos seguintes:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Crie o cluster respondendo aos prompts.

   Os prompts são semelhantes aos seguintes:

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


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Adicione licenças, configure um SVM de Administração de clusters e insira informações de DNS respondendo aos prompts.

   Os prompts são semelhantes aos seguintes:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Ative o failover de armazenamento e configure o nó respondendo aos prompts.

   Os prompts são semelhantes aos seguintes:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Conclua a configuração do nó, mas não crie agregados de dados.

Você pode usar o Gerenciador de sistema do ONTAP, apontando seu navegador da Web para o endereço IP de gerenciamento de cluster (https://172.17.12.153).

"Gerenciamento de clusters usando o Gerenciador de sistemas (ONTAP 9.7 e anteriores)"

"Gerenciador do sistema ONTAP (versão 9,7 e posterior)"

g. Configure o processador de serviço (SP):

"Configure a rede SP/BMC"

"Use um processador de serviço com o Gerenciador do sistema - ONTAP 9.7 e anterior"

3. Inicie o próximo controlador e junte-o ao cluster, seguindo as instruções.
4. Confirme se os nós estão configurados no modo de alta disponibilidade:

```
storage failover show -fields mode
```

Caso contrário, você deve configurar o modo HA em cada nó e reinicializar os nós:

```
storage failover modify -mode ha -node localhost
```

O estado de configuração esperado de failover de HA e storage é o seguinte:

- O modo HA está configurado, mas o failover de armazenamento não está ativado.
- A funcionalidade de aquisição DE HA está desativada.
- As interfaces HA estão offline.
- O modo HA, o failover de storage e as interfaces são configurados posteriormente no processo.

5. Confirme se você tem quatro portas configuradas como interconexões de cluster:

```
network port show
```

As interfaces IP MetroCluster não estão configuradas no momento e não aparecem na saída do comando.

O exemplo a seguir mostra duas portas de cluster no node_A_1:

```
cluster_A::*> network port show -role cluster


Node: node_A_1


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
```

```
false


4 entries were displayed.
```

6. Repita estas etapas no cluster de parceiros.

O que fazer a seguir

Retorne à interface da linha de comando ONTAP e conclua a configuração do MetroCluster executando as tarefas a seguir.

Configuração dos clusters em uma configuração do MetroCluster

É necessário fazer peer nos clusters, espelhar os agregados raiz, criar um agregado de dados espelhados e, em seguida, emitir o comando para implementar as operações do MetroCluster.

Sobre esta tarefa

Antes de executar `metrocluster configure`o , o modo HA e o espelhamento de DR não estão ativados e você pode ver uma mensagem de erro relacionada a esse comportamento esperado. Você ativa o modo HA e o espelhamento de DR mais tarde quando executa o comando `metrocluster configure` para implementar a configuração.

Desativar a atribuição automática de condução (se estiver a efetuar a atribuição manual no ONTAP 9.4)

No ONTAP 9.4, se a configuração IP do MetroCluster tiver menos de quatro compartimentos de storage externos por local, desative a atribuição automática de unidade em todos os nós e atribua unidades manualmente.

Sobre esta tarefa

Esta tarefa não é necessária no ONTAP 9.5 e posterior.

Essa tarefa não se aplica a um sistema AFF A800 com compartimento interno e sem compartimentos externos.

"Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior"

Passos

1. Desativar a atribuição automática de condução:

```
storage disk option modify -node <node_name> -autoassign off
```

2. Você precisa emitir este comando em todos os nós na configuração IP do MetroCluster.

Verificando a atribuição de unidades do pool 0

Você deve verificar se as unidades remotas estão visíveis para os nós e foram atribuídas corretamente.

Sobre esta tarefa

A atribuição automática depende do modelo da plataforma do sistema de storage e do arranjo do compartimento de unidades.

"Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior"

Passos

1. Verifique se as unidades do pool 0 são atribuídas automaticamente:

   ```
   disk show
   ```

   O exemplo a seguir mostra a saída "cluster_A" para um sistema AFF A800 sem prateleiras externas.

   Um quarto (8 unidades) foi atribuído automaticamente a "node_A_1" e um quarto foi atribuído automaticamente a "node_A_2". As unidades restantes serão unidades remotas (pool 1) para "node_B_1" e "node_B_2".

   ```
   cluster_A::*> disk show
                    Usable      Disk      Container           Container
   Disk             Size        Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   ```

```
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

O exemplo a seguir mostra a saída "cluster_B":

```
cluster_B::> disk show
                  Usable     Disk              Container   Container
Disk              Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
```

```
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_B_2
node_B_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_B_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_B_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_B_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_B_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_B_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_B_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_B_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_B_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_B_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_B_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_B_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_B_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_B_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_B_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_B_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.

cluster_B::>
```

Peering dos clusters

Os clusters na configuração do MetroCluster precisam estar em um relacionamento de mesmo nível para que possam se comunicar uns com os outros e executar o espelhamento de dados essencial para a recuperação de desastres do MetroCluster.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

"Considerações ao usar portas dedicadas"

"Considerações ao compartilhar portas de dados"

Configurando LIFs entre clusters para peering de cluster

É necessário criar LIFs entre clusters nas portas usadas para comunicação entre os clusters de parceiros da MetroCluster. Você pode usar portas dedicadas ou portas que também têm tráfego de dados.

Configurando LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede em "cluster01":

   ```
   cluster01::> network port show
                                                                  Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

```
network interface show -fields home-port,curr-port
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que as portas "e0e" e "e0f" não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

```
network interface failover-groups create -vserver <system_svm> -failover-group
<failover_group> -targets <physical_or_logical_ports>
```

O exemplo a seguir atribui portas "e0e" e" e0f" ao grupo de failover "intercluster01" no sistema "SVMcluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

```
network interface failover-groups show
```

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

No ONTAP 9.6 e posterior, execute:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

No ONTAP 9.5 e anteriores, execute:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" no grupo de failover "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

No ONTAP 9.6 e posterior, execute:

```
network interface show -service-policy default-intercluster
```

No ONTAP 9.5 e anteriores, execute:

```
network interface show -role intercluster
```

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verifique se as LIFs entre clusters são redundantes:

No ONTAP 9.6 e posterior, execute:

```
network interface show -service-policy default-intercluster -failover
```

No ONTAP 9.5 e anteriores, execute:

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "SVMe0e" irão falhar para a porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Informações relacionadas

"Considerações ao usar portas dedicadas"

Configurando LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede em "cluster01":

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Criar LIFs entre clusters no sistema:

No ONTAP 9.6 e posterior, execute:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask>
```

No ONTAP 9.5 e anteriores, execute:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

No ONTAP 9.6 e posterior, execute:

```
network interface show -service-policy default-intercluster
```

No ONTAP 9.5 e anteriores, execute:

```
network interface show -role intercluster
```

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

No ONTAP 9.6 e posterior, execute:

```
network interface show -service-policy default-intercluster -failover
```

No ONTAP 9.5 e anteriores, execute:

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "e0c" falharão para a porta "e0d".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Informações relacionadas

"Considerações ao compartilhar portas de dados"

Criando um relacionamento de cluster peer

Você pode usar o comando cluster peer create para criar uma relação de peer entre um cluster local e remoto. Após a criação do relacionamento de pares, você pode executar o cluster peer create no cluster remoto para autenticá-lo no cluster local.

Sobre esta tarefa

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior.

Passos

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

   ```
   cluster peer create -generate-passphrase -offer-expiration <MM/DD/YYYY
   HH:MM:SS|1…7days|1…168hours> -peer-addrs <peer_lif_ip_addresses> -ipspace
   <ipspace>
   ```

   Se você especificar ambos `-generate-passphrase` e `-peer-addrs`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addrs` poderá usar a senha gerada.

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um relacionamento de peer de cluster em um cluster remoto não especificado:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. No cluster de origem, autentique o cluster de origem no cluster de destino:

   `cluster peer create -peer-addrs <peer_lif_ip_addresses> -ipspace <ipspace>`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autentica o cluster local para o cluster remoto em endereços IP de LIF "192.140.112.101" e "192.140.112.102":

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                               Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

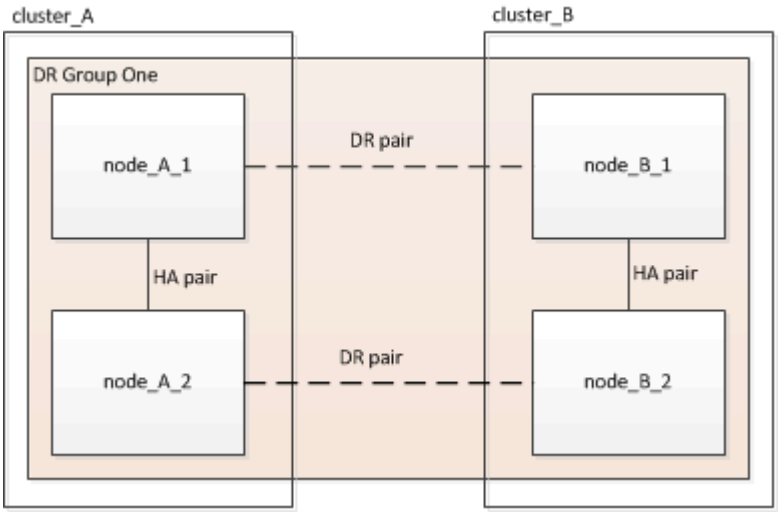
Criando o grupo DR

É necessário criar relações de grupo de recuperação de desastres (DR) entre os clusters.

Sobre esta tarefa

Execute este procedimento em um dos clusters na configuração do MetroCluster para criar as relações de DR entre os nós nos dois clusters.

As relações de DR não podem ser alteradas após a criação dos grupos de DR.



Passos

1. Verifique se os nós estão prontos para a criação do grupo DR inserindo o seguinte comando em cada nó:

   ```
   metrocluster configuration-settings show-status
   ```

   O comando output deve mostrar que os nós estão prontos:

   ```
   cluster_A::> metrocluster configuration-settings show-status
   Cluster                   Node          Configuration Settings Status
   ------------------------- -------------
   -------------------------------
   cluster_A                 node_A_1      ready for DR group create
                             node_A_2      ready for DR group create
   2 entries were displayed.
   ```

   ```
   cluster_B::> metrocluster configuration-settings show-status
   Cluster                   Node          Configuration Settings Status
   ------------------------- -------------
   -------------------------------
   cluster_B                 node_B_1      ready for DR group create
                             node_B_2      ready for DR group create
   2 entries were displayed.
   ```

2. Crie o grupo DR:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   <partner_cluster_name> -local-node <local_node_name> -remote-node
   ```

`<remote_node_name>`

Este comando é emitido apenas uma vez. Isso não precisa ser repetido no cluster de parceiros. No comando, especifique o nome do cluster remoto e o nome de um nó local e um nó no cluster de parceiros.

Os dois nós especificados são configurados como parceiros de DR e os outros dois nós (que não são especificados no comando) são configurados como o segundo par de DR no grupo de DR. Essas relações não podem ser alteradas depois de inserir este comando.

O comando a seguir cria esses pares de DR:

- node_A_1 e node_B_1
- node_A_2 e node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Configuração e conexão das interfaces IP do MetroCluster

É necessário configurar as interfaces IP do MetroCluster usadas para replicação do storage de cada nó e do cache não volátil. Em seguida, você estabelece as conexões usando as interfaces IP do MetroCluster. Isso cria conexões iSCSI para replicação de armazenamento.

> O IP MetroCluster e as portas do switch conetado não ficam online até que você crie as interfaces IP MetroCluster.

Sobre esta tarefa

- É necessário criar duas interfaces para cada nó. As interfaces devem estar associadas às VLANs definidas no arquivo MetroCluster RCF.
- Dependendo da versão do ONTAP, você pode alterar algumas propriedades da interface IP do MetroCluster após a configuração inicial. "Modifique as propriedades de uma interface IP do MetroCluster"Consulte para obter detalhes sobre o que é suportado.
- Você deve criar todas as portas "A" da interface IP do MetroCluster na mesma VLAN e todas as portas "B" da interface IP do MetroCluster na outra VLAN. "Considerações para a configuração IP do MetroCluster"Consulte a .
- A partir do ONTAP 9.9,1, se você estiver usando uma configuração da camada 3, você também deve especificar o `-gateway` parâmetro ao criar interfaces IP do MetroCluster. "Considerações para redes de grande área da camada 3"Consulte a .

  Certas plataformas usam uma VLAN para a interface IP do MetroCluster. Por padrão, cada uma das duas portas usa uma VLAN diferente: 10 e 20.

  Se suportado, você também pode especificar uma VLAN diferente (não padrão) maior que 100 (entre 101 e 4095) usando o `-vlan-id` parâmetro no `metrocluster configuration-settings interface create` comando.

  As seguintes plataformas **não** suportam o `-vlan-id` parâmetro:

  - FAS8200 e AFF A300

- AFF A320
- FAS9000 e AFF A700
- AFF C800, ASA C800, AFF A800 e ASA A800

  Todas as outras plataformas suportam o `-vlan-id` parâmetro.

  As atribuições de VLAN padrão e válidas dependem se a plataforma suporta o `-vlan-id` parâmetro:

Plataformas que suportam <code>-vlan-id</code>

VLAN predefinida:

- Quando o `-vlan-id` parâmetro não é especificado, as interfaces são criadas com VLAN 10 para as portas "A" e VLAN 20 para as portas "B".
- A VLAN especificada deve corresponder à VLAN selecionada no RCF.

Intervalos de VLAN válidos:

- VLAN 10 e 20 padrão
- VLANs 101 e superior (entre 101 e 4095)

Plataformas que não suportam <code>-vlan-id</code>

VLAN predefinida:

- Não aplicável. A interface não requer que uma VLAN seja especificada na interface MetroCluster. A porta do switch define a VLAN que é usada.

Intervalos de VLAN válidos:

- Todas as VLANs não explicitamente excluídas ao gerar o RCF. O RCF alerta-o se a VLAN for inválida.

- As portas físicas usadas pelas interfaces IP do MetroCluster dependem do modelo da plataforma. "Cable os switches IP MetroCluster"Consulte para obter informações sobre a utilização da porta do seu sistema.
- Os seguintes endereços IP e sub-redes são usados nos exemplos:

Nó	Interface	Endereço IP	Sub-rede
node_A_1	Interface IP MetroCluster 1	10.1.1.1	10,1.1/24
Interface IP MetroCluster 2	10.1.2.1	10,1.2/24	node_A_2
Interface IP MetroCluster 1	10.1.1.2	10,1.1/24	Interface IP MetroCluster 2
10.1.2.2	10,1.2/24	node_B_1	Interface IP MetroCluster 1

10.1.1.3	10,1.1/24	Interface IP MetroCluster 2	10.1.2.3
10,1.2/24	node_B_2	Interface IP MetroCluster 1	10.1.1.4
10,1.1/24	Interface IP MetroCluster 2	10.1.2.4	10,1.2/24

- Este procedimento utiliza os seguintes exemplos:

  As portas para um sistema AFF A700 ou FAS9000 (E5A e e5b).

  As portas de um sistema AFF A220 mostram como usar o `-vlan-id` parâmetro em uma plataforma suportada.

  Configure as interfaces nas portas corretas para o modelo da sua plataforma.

Passos

1. Confirme se cada nó tem atribuição automática de disco ativada:

   `storage disk option show`

   A atribuição automática de disco atribuirá o pool 0 e o pool 1 discos, de acordo com o compartimento.

   A coluna atribuição automática indica se a atribuição automática de disco está ativada.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

2. Verifique se você pode criar interfaces IP MetroCluster nos nós:

   `metrocluster configuration-settings show-status`

   Todos os nós devem estar prontos:

```
Cluster       Node          Configuration Settings Status
----------    -----------   --------------------------------
cluster_A
              node_A_1      ready for interface create
              node_A_2      ready for interface create
cluster_B
              node_B_1      ready for interface create
              node_B_2      ready for interface create
4 entries were displayed.
```

3. Crie as interfaces em node_A_1.

   a. Configure a interface na porta "E5A" em "node_A_1":

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      O exemplo a seguir mostra a criação da interface na porta "E5A" em "node_A_1" com endereço IP "10,1.1,1":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
      10.1.1.1 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

      Em modelos de plataforma que suportam VLANs para a interface IP do MetroCluster, você pode incluir o `-vlan-id` parâmetro se não quiser usar os IDs de VLAN padrão. O exemplo a seguir mostra o comando para um sistema AFF A220 com um ID de VLAN de 120:

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
      10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

   b. Configure a interface na porta "e5b" em "node_A_1":

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
      -netmask <netmask>
      ```

      O exemplo a seguir mostra a criação da interface na porta "e5b" em "node_A_1" com endereço IP "10,1.2,1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Você pode verificar se essas interfaces estão presentes usando o `metrocluster configuration-settings interface show` comando.

4. Crie as interfaces em node_A_2.

   a. Configure a interface na porta "E5A" em "node_A_2":

      `metrocluster configuration-settings interface create -cluster-name <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address> -netmask <netmask>`

      O exemplo a seguir mostra a criação da interface na porta "E5A" em "node_A_2" com endereço IP "10,1.1,2":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
      10.1.1.2 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

   b. Configure a interface na porta "e5b" em "node_A_2":

      `metrocluster configuration-settings interface create -cluster-name <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address> -netmask <netmask>`

      O exemplo a seguir mostra a criação da interface na porta "e5b" em "node_A_2" com endereço IP "10,1.2,2":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
      10.1.2.2 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

      Em modelos de plataforma que suportam VLANs para a interface IP do MetroCluster, você pode incluir o `-vlan-id` parâmetro se não quiser usar os IDs de VLAN padrão. O exemplo a seguir mostra o comando para um sistema AFF A220 com um ID de VLAN de 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Crie as interfaces em "node_B_1".

   a. Configure a interface na porta "E5A" em "node_B_1":

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      O exemplo a seguir mostra a criação da interface na porta "E5A" em "node_B_1" com endereço IP "10,1.1,3":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_B -home-node node_B_1 -home-port e5a -address
      10.1.1.3 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.cluster_B::>
      ```

   b. Configure a interface na porta "e5b" em "node_B_1":

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
      -netmask <netmask>
      ```

      O exemplo a seguir mostra a criação da interface na porta "e5b" em "node_B_1" com endereço IP "10,1.2,3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Crie as interfaces em "node_B_2".

   a. Configure a interface na porta E5A no node_B_2:

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      O exemplo a seguir mostra a criação da interface na porta "E5A" em "node_B_2" com endereço IP "10,1.1,4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configure a interface na porta "e5b" em "node_B_2":

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

O exemplo a seguir mostra a criação da interface na porta "e5b" em "node_B_2" com endereço IP "10,1.2,4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Verifique se as interfaces foram configuradas:

```
metrocluster configuration-settings interface show
```

O exemplo a seguir mostra que o estado de configuração para cada interface está concluído.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                 Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- --------- ----------
1     cluster_A  node_A_1
                  Home Port: e5a
                       10.1.1.1     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.1     255.255.255.0   -         completed
                  node_A_2
                  Home Port: e5a
                       10.1.1.2     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                  Home Port: e5a
                       10.1.1.3     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.3     255.255.255.0   -         completed
                  node_B_2
                  Home Port: e5a
                       10.1.1.4     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Verifique se os nós estão prontos para conetar as interfaces MetroCluster:

   `metrocluster configuration-settings show-status`

   O exemplo a seguir mostra todos os nós no estado "pronto para conexão":

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Estabeleça as ligações:
`metrocluster configuration-settings connection connect`

   Se você estiver executando uma versão anterior ao ONTAP 9.10,1, os endereços IP não poderão ser alterados depois de emitir este comando.

   O exemplo a seguir mostra que o cluster_A está conetado com êxito:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Verifique se as conexões foram estabelecidas:

    `metrocluster configuration-settings show-status`

    O status das configurações para todos os nós deve ser concluído:

```
Cluster       Node          Configuration Settings Status
----------    -----------   --------------------------------
cluster_A
              node_A_1      completed
              node_A_2      completed
cluster_B
              node_B_1      completed
              node_B_2      completed
4 entries were displayed.
```

11. Verifique se as conexões iSCSI foram estabelecidas:

    a. Mude para o nível de privilégio avançado:

       `set -privilege advanced`

       Você precisa responder `y` quando for solicitado a continuar no modo avançado e você vir o prompt do modo avançado (`*>`).

    b. Apresentar as ligações:

       `storage iscsi-initiator show`

       Em sistemas que executam o ONTAP 9.5, existem oito iniciadores IP MetroCluster em cada cluster que devem aparecer na saída.

       Em sistemas que executam o ONTAP 9.4 e anteriores, há quatro iniciadores IP MetroCluster em cada cluster que devem aparecer na saída.

       O exemplo a seguir mostra os oito iniciadores IP do MetroCluster em um cluster executando o ONTAP 9.5:

```
cluster_A::*> storage iscsi-initiator show
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
-------------------------------- --------

cluster_A-01
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
               mccip-aux-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
               mccip-aux-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
               mccip-aux-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
               mccip-pri-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-pri-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-b-initiator2
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-aux-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-b-initiator2
```

```
                  10.227.95.165:65200     prod507.com.company:cdcd88
up/up
     dr_partner
              mccip-pri-a-initiator
                  10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-pri-a-initiator2
                  10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-pri-b-initiator
                  10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-pri-b-initiator2
                  10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

a. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

12. Verifique se os nós estão prontos para a implementação final da configuração do MetroCluster:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_A
              node_A_1          ready to configure -     -
              node_A_2          ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_B
              node_B_1          ready to configure -     -
              node_B_2          ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Verificando ou executando manualmente a atribuição de unidades do pool 1

Dependendo da configuração de armazenamento, você deve verificar a atribuição da unidade do pool 1 ou atribuir manualmente unidades ao pool 1 para cada nó na configuração IP do MetroCluster. O procedimento utilizado depende da versão do ONTAP que está a utilizar.

Tipo de configuração	Procedimento
Os sistemas atendem aos requisitos de atribuição automática de acionamento ou, se estiver executando o ONTAP 9.3, foram recebidos de fábrica.	Verificando a atribuição de discos para discos do pool 1
A configuração inclui três gavetas ou, se contiver mais de quatro gavetas, tem um múltiplo desigual de quatro gavetas (por exemplo, sete gavetas) e está executando o ONTAP 9.5.	Atribuição manual de unidades para o pool 1 (ONTAP 9.4 ou posterior)
A configuração não inclui quatro gavetas de storage por local e está executando o ONTAP 9.4	Atribuição manual de unidades para o pool 1 (ONTAP 9.4 ou posterior)
Os sistemas não foram recebidos de fábrica e estão executando o ONTAP 9.3Systems recebido de fábrica são pré-configurados com unidades atribuídas.	Atribuição manual de discos para o pool 1 (ONTAP 9.3)

Verificando a atribuição de discos para discos do pool 1

Você deve verificar se os discos remotos estão visíveis para os nós e foram atribuídos corretamente.

Antes de começar

Você deve esperar pelo menos dez minutos para que a atribuição automática do disco seja concluída após as interfaces IP do MetroCluster e as conexões terem sido criadas com o `metrocluster configuration-settings connection connect` comando.

A saída de comando mostrará nomes de disco na forma: Node-name:0m.i1.0L1

"Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior"

Passos

1. Verifique se os discos do pool 1 estão atribuídos automaticamente:

   `disk show`

   A saída a seguir mostra a saída para um sistema AFF A800 sem prateleiras externas.

   A atribuição automática de unidade atribuiu um quarto (8 unidades) a "node_A_1" e um quarto a "node_A_2". As unidades restantes serão discos remotos (pool 1) para "node_B_1" e "node_B_2".

```
cluster_B::> disk show -host-adapter 0m -owner node_B_2
                     Usable     Disk              Container   Container
Disk                 Size       Shelf Bay Type    Type        Name
Owner
```

```
---------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_2:0m.i0.2L4  894.0GB    0     29  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L3  894.0GB    0     28  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L9  894.0GB    0     24  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
node_B_2
8 entries were displayed.

cluster_B::> disk show -host-adapter 0m -owner node_B_1
                     Usable     Disk              Container   Container
Disk                 Size       Shelf Bay Type    Type        Name
Owner
----------------     ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
node_B_1
node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
                     Usable     Disk              Container   Container
```

```
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
```

```
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
```

```
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
```

```
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Atribuição manual de unidades para o pool 1 (ONTAP 9.4 ou posterior)

Se o sistema não tiver sido pré-configurado de fábrica e não atender aos requisitos de atribuição automática de unidades, você deverá atribuir manualmente as unidades 1 do pool remoto.

Sobre esta tarefa

Este procedimento aplica-se às configurações que executam o ONTAP 9.4 ou posterior.

Os detalhes para determinar se o sistema requer atribuição manual de disco estão incluídos no "Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior".

Quando a configuração inclui apenas duas gavetas externas por local, o pool de 1 unidades para cada local deve ser compartilhado a partir do mesmo compartimento, conforme mostrado nos exemplos a seguir:

- Node_A_1 recebe unidades nos compartimentos 0-11 no site_B-shelf_2 (remoto)
- Node_A_2 recebe unidades nos compartimentos 12-23 no site_B-shelf_2 (remoto)

Passos

1. A partir de cada nó na configuração IP do MetroCluster, atribua unidades remotas ao pool 1.

   a. Exiba a lista de unidades não atribuídas:

      ```
      disk show -host-adapter 0m -container-type unassigned
      ```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Atribua a propriedade de unidades remotas (0m) ao pool 1 do primeiro nó (por exemplo, node_A_1):

`disk assign -disk <disk-id> -pool 1 -owner <owner_node_name>`

`disk-id` deve identificar uma unidade em uma gaveta remota de `owner_node_name`.

c. Confirme se as unidades foram atribuídas ao pool 1:

`disk show -host-adapter 0m -container-type unassigned`

> ⓘ A ligação iSCSI utilizada para aceder às unidades remotas é apresentada como dispositivo 0m.

A saída a seguir mostra que as unidades na gaveta 23 foram atribuídas porque não aparecem mais na lista de unidades não atribuídas:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Repita estas etapas para atribuir unidades de pool 1 ao segundo nó no local A (por exemplo, "node_A_2").

b. Repita estes passos no local B..

Atribuição manual de discos para o pool 1 (ONTAP 9.3)

Se você tiver pelo menos duas gavetas de disco para cada nó, use a funcionalidade de atribuição automática do ONTAP para atribuir automaticamente os discos remotos (pool1).

Antes de começar

Primeiro, você deve atribuir um disco na gaveta ao pool 1. Em seguida, o ONTAP atribui automaticamente o restante dos discos na gaveta ao mesmo pool.

Sobre esta tarefa

Este procedimento aplica-se às configurações que executam o ONTAP 9.3.

Esse procedimento só pode ser usado se você tiver pelo menos duas gavetas de disco para cada nó, o que permite a atribuição automática de discos no nível de compartimento.

Se você não puder usar a atribuição automática no nível do compartimento, você deverá atribuir manualmente os discos remotos para que cada nó tenha um pool remoto de discos (pool 1).

O recurso de atribuição automática de disco do ONTAP atribui os discos de acordo com o compartimento. Por exemplo:

- Todos os discos no site_B-shelf_2 são atribuídos automaticamente a pool1 de node_A_1
- Todos os discos no site_B-shelf_4 são atribuídos automaticamente a pool1 de node_A_2
- Todos os discos no site_A-shelf_2 são atribuídos automaticamente a pool1 de node_B_1
- Todos os discos no site_A-shelf_4 são atribuídos automaticamente a pool1 de node_B_2

Você deve "semear" a atribuição automática especificando um único disco em cada prateleira.

Passos

1. A partir de cada nó na configuração IP do MetroCluster, atribua um disco remoto ao pool 1.

   a. Exibir a lista de discos não atribuídos:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   ```
   cluster_A::> disk show -host-adapter 0m -container-type unassigned
                        Usable           Disk    Container   Container
   Disk                   Size Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   6.23.0                    -    23   0 SSD     unassigned  -         -
   6.23.1                    -    23   1 SSD     unassigned  -         -
   .
   .
   .
   node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
   node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
   .
   .
   .
   48 entries were displayed.

   cluster_A::>
   ```

   b. Selecione um disco remoto (0m) e atribua a propriedade do disco ao pool 1 do primeiro nó (por exemplo, "node_A_1"):

   ```
   disk assign -disk <disk_id> -pool 1 -owner <owner_node_name>
   ```

   O `disk-id` deve identificar um disco em uma gaveta remota de `owner_node_name`.

   O recurso de atribuição automática de disco ONTAP atribui todos os discos no compartimento remoto que contém o disco especificado.

   c. Depois de esperar pelo menos 60 segundos para que a atribuição automática do disco ocorra, verifique se os discos remotos na gaveta foram atribuídos automaticamente ao pool 1:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   > ⓘ A ligação iSCSI utilizada para aceder aos discos remotos é apresentada como dispositivo 0m.

   A saída a seguir mostra que os discos na gaveta 23 agora foram atribuídos e não aparecem mais:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Repita estas etapas para atribuir discos do pool 1 ao segundo nó no local A (por exemplo, "node_A_2").

b. Repita estes passos no local B..

Habilitando a atribuição automática de acionamento no ONTAP 9.4

Sobre esta tarefa

No ONTAP 9.4, se você desativou a atribuição automática de unidade como indicado anteriormente neste procedimento, você deve reativá-la em todos os nós.

"Considerações para atribuição automática de acionamento e sistemas ADP no ONTAP 9.4 e posterior"

Passos

1. Ativar atribuição automática de condução:

   ```
   storage disk option modify -node <node_name> -autoassign on
   ```

   Você deve emitir este comando em todos os nós na configuração IP do MetroCluster.

Espelhamento dos agregados de raiz

É necessário espelhar os agregados raiz para fornecer proteção de dados.

Sobre esta tarefa

Por padrão, o agregado raiz é criado como agregado do tipo RAID-DP. Você pode alterar o agregado raiz de RAID-DP para o agregado do tipo RAID4. O comando a seguir modifica o agregado raiz para o agregado do tipo RAID4:

```
storage aggregate modify –aggregate <aggr_name> -raidtype raid4
```

> Em sistemas que não sejam ADP, o tipo RAID do agregado pode ser modificado do RAID-DP padrão para RAID4 antes ou depois que o agregado é espelhado.

Passos

1. Espelhar o agregado raiz:

   ```
   storage aggregate mirror <aggr_name>
   ```

   O comando a seguir espelha o agregado raiz para "controller_A_1":

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Isso reflete o agregado, por isso consiste em um Plex local e um Plex remoto localizado no local remoto de MetroCluster.

2. Repita a etapa anterior para cada nó na configuração do MetroCluster.

Informações relacionadas

"Gerenciamento de storage lógico"

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

Sobre esta tarefa

- Você deve saber quais unidades serão usadas no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.
- As unidades são de propriedade de um nó específico; quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.

  Em sistemas que usam ADP, agregados são criados usando partições nas quais cada unidade é

particionada em partições P1, P2 e P3.

- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.

  "Gerenciamento de disco e agregado"

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   ```
   storage disk show -spare -owner <node_name>
   ```

2. Criar o agregado:

   ```
   storage aggregate create -mirror true
   ```

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para garantir que o agregado seja criado em um nó específico, use o `-node` parâmetro ou especifique as unidades que são de propriedade desse nó.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas que devem ser adicionadas ao agregado
   - Número de unidades a incluir

     > Na configuração mínima suportada, na qual um número limitado de unidades está disponível, você deve usar a opção force-small-Aggregate para permitir a criação de um agregado RAID-DP de três discos.

   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades que podem ser incluídas em um grupo RAID
   - Se unidades com RPM diferentes são permitidas para obter mais informações sobre essas opções, consulte a página de manual criação de agregados de armazenamento.

     O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

```
storage aggregate show-status -aggregate <aggregate-name>
```

Implementando a configuração do MetroCluster

Você deve executar o `metrocluster configure` comando para iniciar a proteção de dados em uma configuração do MetroCluster.

Sobre esta tarefa

- Deve haver pelo menos dois agregados de dados espelhados não-raiz em cada cluster.

  Você pode verificar isso com o `storage aggregate show` comando.

  > Se você quiser usar um único agregado de dados espelhados, consulte Passo 1 para obter instruções.

- O estado ha-config dos controladores e chassis deve ser "mccip".

Você emite o `metrocluster configure` comando uma vez em qualquer um dos nós para ativar a configuração do MetroCluster. Você não precisa emitir o comando em cada um dos sites ou nós, e não importa em qual nó ou site você escolher emitir o comando.

`metrocluster configure`O comando emparelhará automaticamente os dois nós com as IDs de sistema mais baixas em cada um dos dois clusters como parceiros de recuperação de desastres (DR). Em uma configuração de MetroCluster de quatro nós, há dois pares de parceiros de DR. O segundo par de DR é criado a partir dos dois nós com IDs de sistema mais altas.

> Você deve configurar o OKM (Onboard Key Manager) ou o gerenciamento de chaves externas antes de executar o comando `metrocluster configure`.

Passos

1. Configure o MetroCluster no seguinte formato:

Se a sua configuração do MetroCluster tiver…	Então faça isso…
Vários agregados de dados	A partir do prompt de qualquer nó, configure o MetroCluster: `metrocluster configure <node_name>`

Um único agregado de dados espelhados	a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado: `set -privilege advanced` Você precisa responder `y` quando for solicitado a continuar no modo avançado e você vir o prompt do modo avançado (*>). b. Configure o MetroCluster com o `-allow-with-one-aggregate true` parâmetro: `metrocluster configure -allow-with-one-aggregate true <node_name>` c. Voltar ao nível de privilégio de administrador: `set -privilege admin`

A prática recomendada é ter vários agregados de dados. Se o primeiro grupo de DR tiver apenas um agregado e quiser adicionar um grupo de DR com um agregado, mova o volume de metadados do agregado de dados único. Para obter mais informações sobre este procedimento, "Movimentação de um volume de metadados nas configurações do MetroCluster"consulte .

O comando a seguir habilita a configuração do MetroCluster em todos os nós do grupo DR que contém "controller_A_1":

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verifique o status da rede no local A:

   `network port show`

   O exemplo a seguir mostra o uso da porta de rede em uma configuração MetroCluster de quatro nós:

```
cluster_A::> network port show
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.

   a. Verifique a configuração do local A:

      `metrocluster show`

      ```
      cluster_A::> metrocluster show

      Configuration: IP fabric

      Cluster                   Entry Name          State
      ------------------------- ------------------- -----------
       Local: cluster_A         Configuration state configured
                                Mode                normal
      Remote: cluster_B         Configuration state configured
                                Mode                normal
      ```

   b. Verifique a configuração a partir do local B:

      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

4. Para evitar possíveis problemas com o espelhamento de memória não volátil, reinicie cada um dos quatro nós:

   `node reboot -node <node_name> -inhibit-takeover true`

5. Emita o `metrocluster show` comando em ambos os clusters para verificar novamente a configuração.

Configurando o segundo grupo de DR em uma configuração de oito nós

Repita as tarefas anteriores para configurar os nós no segundo grupo de DR.

Criação de agregados de dados sem espelhamento

Você pode, opcionalmente, criar agregados de dados sem espelhamento para dados que não exigem o espelhamento redundante fornecido pelas configurações do MetroCluster.

Sobre esta tarefa

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode verificar se o tipo de unidade correto está selecionado.

> Nas configurações IP do MetroCluster, agregados remotos sem espelhamento não são acessíveis após um switchover

> Os agregados sem espelhamento devem ser locais para o nó que os possui.

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.
- *Gerenciamento de discos e agregados* contém mais informações sobre o espelhamento de agregados.

Passos

1. Ativar a implantação de agregados sem espelhamento:

   `metrocluster modify -enable-unmirrored-aggr-deployment`

```
true
```

2. Verifique se a atribuição automática de disco está desativada:

```
disk option show
```

3. Instale e faça o cabeamento das gavetas de disco que conterão os agregados sem espelhamento.

   Você pode usar os procedimentos na documentação de instalação e configuração para sua plataforma e compartimentos de disco.

   "Documentação dos sistemas de hardware da ONTAP"

4. Atribua manualmente todos os discos na nova gaveta ao nó apropriado:

```
disk assign -disk <disk_id> -owner <owner_node_name>
```

5. Criar o agregado:

```
storage aggregate create
```

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para verificar se o agregado é criado em um nó específico, você deve usar o parâmetro -node ou especificar unidades que são de propriedade desse nó.

   Você também precisa garantir que você inclua somente unidades na gaveta sem espelhamento do agregado.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
   - Número de unidades a incluir
   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
   - Se unidades com RPM diferentes são permitidas

     Para obter mais informações sobre essas opções, consulte a página de manual criar agregado de armazenamento.

     O comando a seguir cria um agregado sem espelhamento com 10 discos:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate <aggregate_name>`

7. Desativar a implantação de agregados sem espelhamento:

   `metrocluster modify -enable-unmirrored-aggr-deployment false`

8. Verifique se a atribuição automática de disco está ativada:

   `disk option show`

Informações relacionadas

"Gerenciamento de disco e agregado"

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente.

Sobre esta tarefa

Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster.

Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Os comandos subsequentes `metrocluster check show` não mostram a saída esperada.

Passos

1. Verificar a configuração:

   `metrocluster check run`

   O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Exibir resultados mais detalhados do comando MetroCluster check run mais recente:

```
metrocluster check aggregate show

metrocluster check cluster show

metrocluster check config-replication show

metrocluster check lif show

metrocluster check node show
```

> Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

```
cluster_A::> metrocluster check aggregate show
```

```
Node                Aggregate                Check
Result
---------------     --------------------     ---------------------
---------
controller_A_1      controller_A_1_aggr0
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_1_aggr1
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_1_aggr2
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok


controller_A_2      controller_A_2_aggr0
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_2_aggr1
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_2_aggr2
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
```

```
                                                    ownership-state
ok

18 entries were displayed.
```

O exemplo a seguir mostra a saída do comando MetroCluster check cluster show para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

```
Cluster               Check                                Result
--------------------- ---------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
10 entries were displayed.
```

Informações relacionadas

"Gerenciamento de disco e agregado"

"Gerenciamento de rede e LIF"

A concluir a configuração do ONTAP

Após configurar, ativar e verificar a configuração do MetroCluster, você pode concluir a configuração do cluster adicionando SVMs adicionais, interfaces de rede e outras funcionalidades do ONTAP, conforme necessário.

Configurar criptografia de ponta a ponta

A partir do ONTAP 9.15,1, é possível configurar a criptografia de ponta a ponta para criptografar o tráfego de back-end, como NVlog e dados de replicação de armazenamento, entre os sites em uma configuração IP do MetroCluster.

Sobre esta tarefa

- Você deve ser um administrador de cluster para executar esta tarefa.
- Antes de poder configurar a encriptação de ponta a ponta, tem "Configurar o gerenciamento de chaves externas"de .
- Revise os sistemas suportados e a versão mínima do ONTAP necessária para configurar a criptografia de

ponta a ponta em uma configuração IP do MetroCluster:

Versão mínima de ONTAP	Sistemas suportados
ONTAP 9.15,1	• AFF A400 • FAS8300 • FAS8700

Ative a criptografia de ponta a ponta

Execute as etapas a seguir para habilitar a criptografia de ponta a ponta.

Passos

1. Verifique a integridade da configuração do MetroCluster.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   A operação é executada em segundo plano.

   b. Após `metrocluster check run` a conclusão da operação, execute:

   ```
   metrocluster check show
   ```

   Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

   a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id <id>
```

b. Verifique se não há alertas de saúde:

```
system health alert show
```

2. Verifique se o gerenciamento de chaves externas está configurado em ambos os clusters:

```
security key-manager external show-status
```

3. Habilite a criptografia de ponta a ponta para cada grupo de DR:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Exemplo

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Repita esta etapa para cada grupo de DR na configuração.

4. Verifique se a criptografia de ponta a ponta está ativada:

```
metrocluster node show -fields is-encryption-enabled
```

Exemplo

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

Desative a criptografia de ponta a ponta

Execute as etapas a seguir para desativar a criptografia de ponta a ponta.

Passos

1. Verifique a integridade da configuração do MetroCluster.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   A operação é executada em segundo plano.

   b. Após `metrocluster check run` a conclusão da operação, execute:

   ```
   metrocluster check show
   ```

   Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id <id>
```

b. Verifique se não há alertas de saúde:

```
system health alert show
```

2. Verifique se o gerenciamento de chaves externas está configurado em ambos os clusters:

```
security key-manager external show-status
```

3. Desative a criptografia de ponta a ponta em cada grupo de DR:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Exemplo

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Repita esta etapa para cada grupo de DR na configuração.

4. Verifique se a criptografia de ponta a ponta está desativada:

```
metrocluster node show -fields is-encryption-enabled
```

Exemplo

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Verificando switchover, cura e switchback

Passo

1. Use os procedimentos para comutação negociada, cura e switchback mencionados no *Guia de gerenciamento e recuperação de desastres do MetroCluster*.

   "Gerenciamento de MetroCluster e recuperação de desastres"

Configurando o software tiebreaker do MetroCluster ou do ONTAP Mediator

Você pode baixar e instalar em um terceiro site o software tiebreaker do MetroCluster ou, a partir do ONTAP 9.7, o Mediador do ONTAP.

Antes de começar

Você precisa ter um host Linux disponível que tenha conetividade de rede para ambos os clusters na configuração do MetroCluster. Os requisitos específicos estão na documentação do MetroCluster Tiebreaker ou do ONTAP Mediator.

Se você estiver se conetando a uma instância existente do tiebreaker ou do ONTAP Mediator, precisará do nome de usuário, senha e endereço IP do serviço tiebreaker ou Mediator.

Se for necessário instalar uma nova instância do Mediador ONTAP, siga as instruções para instalar e configurar o software.

"Configuração do serviço ONTAP Mediator para switchover automático não planejado"

Se for necessário instalar uma nova instância do software tiebreaker, siga o "instruções para instalar e configurar o software".

Sobre esta tarefa

Não é possível usar o software tiebreaker do MetroCluster e o Mediador do ONTAP com a mesma configuração do MetroCluster.

"Considerações sobre o uso do ONTAP Mediator ou do MetroCluster Tiebreaker"

Passo

1. Configure o serviço do ONTAP Mediator ou o software tiebreaker:
   - Se você estiver usando uma instância existente do Mediador ONTAP, adicione o serviço Mediador ONTAP ao ONTAP:

     ```
     metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
     ```

   - Se você estiver usando o software tiebreaker, consulte o "Documentação do desempate".

Protegendo arquivos de backup de configuração

Você pode fornecer proteção adicional para os arquivos de backup de configuração de cluster especificando um URL remoto (HTTP ou FTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster local.

Passo

1. Defina o URL do destino remoto para os arquivos de backup de configuração:

   ```
   system configuration backup settings modify URL-of-destination
   ```

O "Gerenciamento de clusters com a CLI" contém informações adicionais na seção *Gerenciando backups de configuração*.

Configure o software MetroCluster usando o Gerenciador do sistema

Configure um site IP do MetroCluster

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para configurar um site IP do MetroCluster.

Um local do MetroCluster consiste em dois clusters. Normalmente, os clusters estão localizados em diferentes locais geográficos.

Antes de começar

- O sistema já deve estar instalado e cabeado de acordo com o "Instruções de instalação e configuração" fornecido com o sistema.
- As interfaces de rede do cluster devem ser configuradas em cada nó de cada cluster para comunicação intra-cluster.

Atribua um endereço IP de gerenciamento de nó

Sistema Windows

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

Passos

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

Outros sistemas

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

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

Inicialize e configure o cluster

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

Passos

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

   O System Manager descobre automaticamente os nós restantes no cluster.

2. Na janela **Initialize Storage System**, execute o seguinte procedimento:
   a. Insira os dados de configuração da rede de gerenciamento de cluster.
   b. Insira os endereços IP de gerenciamento de nós para todos os nós.
   c. Forneça detalhes de DNS.
   d. Na seção **outro**, marque a caixa de seleção **Use Time Service (NTP)** para adicionar os servidores de horário.

Quando clicar em **Submit**, aguarde até que o cluster seja criado e configurado. Em seguida, ocorre um processo de validação.

O que se segue?

Depois que ambos os clusters tiverem sido configurados, inicializados e configurados, execute o procedimento [Configurar peering IP MetroCluster].

Configure o ONTAP em um novo vídeo de cluster

Configurar o peering IP do MetroCluster

A partir do ONTAP 9.8, você pode gerenciar as operações de configuração IP do MetroCluster com o Gerenciador de sistema. Depois de configurar dois clusters, configure o peering entre eles.

Antes de começar

Configure dois clusters. Consulte "Configure um site IP do MetroCluster"o procedimento.

Determinadas etapas deste processo são executadas por diferentes administradores de sistema localizados nos locais geográficos de cada cluster. Para explicar este processo, os clusters são chamados de "Site A cluster" e "Site B cluster".

Execute o processo de peering do Site A.

Este processo é executado por um administrador de sistema no local A..

Passos

1. Faça login no Site Um cluster.
2. No System Manager, selecione **Dashboard** na coluna de navegação à esquerda para exibir a visão geral do cluster.

   O painel mostra os detalhes deste cluster (Site A). Na seção **MetroCluster**, Site Um cluster é mostrado à esquerda.

3. Clique em **Anexar cluster de parceiros**.
4. Insira os detalhes das interfaces de rede que permitem que os nós no local Um cluster se comuniquem com os nós no cluster do local B.

5. Clique em **Salvar e continuar**.
6. Na janela **Anexar cluster de parceiros**, selecione **não tenho uma senha**. Isso permite gerar uma senha.
7. Copie a senha gerada e compartilhe-a com o administrador do sistema no Site B..
8. Selecione **Fechar**.

Execute o processo de peering do local B.

Este processo é realizado por um administrador de sistema no local B..

Passos

1. Inicie sessão no cluster do local B.
2. No System Manager, selecione **Dashboard** para exibir a visão geral do cluster.

   O painel mostra os detalhes deste cluster (local B). Na seção MetroCluster, o cluster do local B é exibido à esquerda.

3. Clique em **Attach Partner Cluster** para iniciar o processo de peering.
4. Insira os detalhes das interfaces de rede que permitem que os nós no cluster do local B se comuniquem com os nós no cluster do local A.
5. Clique em **Salvar e continuar**.
6. Na janela **Anexar cluster de parceiros**, selecione **tenho uma senha**. Isto permite-lhe introduzir a frase-passe que recebeu do administrador do sistema no local A..
7. Selecione **Peer** para concluir o processo de peering.

O que se segue?

Depois que o processo de peering for concluído com êxito, você configurará os clusters. "Configurar um site IP do MetroCluster"Consulte .

Configurar um site IP do MetroCluster

A partir do ONTAP 9.8, você pode gerenciar as operações de configuração IP do MetroCluster com o Gerenciador de sistema. Isso envolve a configuração de dois clusters, a execução de peering de cluster e a configuração dos clusters.

Antes de começar

Execute os seguintes procedimentos:

- "Configure um site IP do MetroCluster"
- "Configurar o peering IP do MetroCluster"

Configurar a conexão entre clusters

Passos

1. Faça login no System Manager em um dos sites e selecione **Dashboard**.

   Na seção **MetroCluster**, o gráfico mostra os dois clusters configurados e direcionados para os sites do MetroCluster. O cluster a partir do qual está a trabalhar (cluster local) é apresentado à esquerda.

2. Clique em **Configurar MetroCluster**. Nesta janela, execute as seguintes etapas:

a. Os nós de cada cluster na configuração do MetroCluster são mostrados. Use as listas suspensas para selecionar os nós no cluster local que serão parceiros de recuperação de desastres com os nós no cluster remoto.

b. Clique na caixa de verificação se pretender configurar o serviço Mediador ONTAP. "Configure o serviço do Mediador ONTAP"Consulte .

c. Se ambos os clusters tiverem uma licença para ativar a criptografia, a seção **criptografia** será exibida.

   Para ativar a encriptação, introduza uma frase-passe.

d. Clique na caixa de verificação se pretender configurar o MetroCluster com uma rede de camada 3 partilhada.

   Os nós de parceiros de HA e os switches de rede que se conetam aos nós precisam ter uma configuração correspondente.

3. Clique em **Salvar** para configurar os sites do MetroCluster.

   No **Painel**, na seção **MetroCluster**, o gráfico mostra uma marca de seleção no link entre os dois clusters, indicando uma conexão saudável.

Configure o serviço ONTAP Mediator para switchover automático não planejado

Prepare-se para instalar o serviço Mediador ONTAP

Seu ambiente precisa atender a certos requisitos.

Os requisitos a seguir se aplicam a um grupo de recuperação de desastres (grupo de DR). Saiba mais "Grupos DR"sobre o .

- Se você planeja atualizar sua versão Linux, faça isso antes de instalar o serviço Mediador ONTAP mais atual.
- O serviço do ONTAP Mediator e o software tiebreaker do MetroCluster não devem ser usados com a mesma configuração do MetroCluster.
- O Mediador ONTAP deve ser instalado em um host LINUX em um local separado dos sites do MetroCluster.

  A conetividade entre o Mediador ONTAP e cada site deve ser dois domínios de falha separados.

- O serviço Mediador ONTAP pode suportar até cinco configurações de MetroCluster simultaneamente.
- O switchover não planejado automático é suportado no ONTAP 9.7 e posterior.

Requisitos de rede para usar o Mediator em uma configuração MetroCluster

Para instalar o serviço do Mediador ONTAP em uma configuração do MetroCluster, você deve certificar-se de que a configuração atende a vários requisitos de rede.

- Latência

  Latência máxima inferior a 75ms ms (RTT).

O jitter não deve ser mais do que 5ms.

- MTU

  O tamanho da MTU deve ser de pelo menos 1400.

- Perda de pacotes

  Para o tráfego ICMP (Internet Control Message Protocol) e TCP, a perda de pacotes deve ser inferior a 0,01%.

- Largura de banda

  O link entre o serviço Mediator e um grupo DR deve ter pelo menos 20Mbps Gbps de largura de banda.

- Conetividade independente

  É necessária conetividade independente entre cada local e o Mediador ONTAP. Uma falha em um local não deve interromper a conetividade IP entre os outros dois locais não afetados.

Requisitos de host para o Mediador ONTAP em uma configuração MetroCluster

Você deve garantir que a configuração atenda a vários requisitos de host.

- O Mediador ONTAP deve ser instalado em um local externo fisicamente separado dos dois clusters do ONTAP.
- O Mediador ONTAP suporta um número máximo de cinco configurações MetroCluster.
- O ONTAP Mediator não requer mais do que os requisitos mínimos do sistema operacional host para CPU e memória (RAM).
- Além dos requisitos mínimos do sistema operacional host, pelo menos 30GBMB de espaço em disco utilizável adicional devem estar disponíveis.
  - Cada grupo de DR requer até 200MB GB de espaço em disco.

Requisitos de firewall para o ONTAP Mediator

O Mediador ONTAP usa várias portas para se comunicar com serviços específicos.

Se você estiver usando um firewall de terceiros:

- O acesso HTTPS deve estar ativado.
- Ele deve ser configurado para permitir acesso nas portas 31784 e 3260.

  Ao usar o firewall padrão Red Hat ou CentOS, o firewall é configurado automaticamente durante a instalação do Mediator.

A tabela a seguir lista as portas que você deve permitir no firewall:

ⓘ A porta iSCSI só é necessária numa configuração IP MetroCluster.

Porta/serviços	Fonte	Destino	Finalidade

31784/tcp	Interfaces de gerenciamento de clusters do ONTAP	Servidor web ONTAP Mediator	API REST (HTTPS)
3260/tcp	Cluster ONTAP (LIF de dados ou LIF de gerenciamento de dados)	ISCSI do Mediador ONTAP	Ligação de dados iSCSI para caixas de correio

Diretrizes para atualizar o Mediador ONTAP em uma configuração MetroCluster

Se você estiver atualizando o Mediador do ONTAP, você deve atender aos requisitos de versão do Linux e seguir as diretrizes para a atualização.

- O serviço Mediator pode ser atualizado de uma versão imediatamente anterior para a versão atual.
- Todas as versões do Mediator são suportadas em configurações IP do MetroCluster executando o ONTAP 9.7 ou posterior.

"Instale ou atualize o serviço do Mediador ONTAP"

Após a atualização

Depois que a atualização do Mediator e do sistema operacional estiver concluída, você deverá emitir o `storage iscsi-initiator show` comando para confirmar se as conexões do Mediator estão ativas.

Configure o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster

O serviço do Mediador ONTAP deve ser configurado no nó ONTAP para uso em uma configuração IP do MetroCluster.

Antes de começar

- O Mediador ONTAP deve ter sido instalado com sucesso em um local de rede que possa ser acessado por ambos os sites da MetroCluster.

  "Instale ou atualize o serviço do Mediador ONTAP"

- Você deve ter o endereço IP do host que executa o serviço do Mediador ONTAP.
- Você deve ter o nome de usuário e a senha para o serviço do Mediador ONTAP.
- Todos os nós da configuração IP do MetroCluster devem estar online.

> A partir do ONTAP 9.12,1, você pode ativar o recurso de comutação forçada automática MetroCluster em uma configuração IP MetroCluster. Este recurso é uma extensão da comutação não planejada assistida por Mediator. Antes de ativar esta funcionalidade, reveja o "Riscos e limitações do uso do switchover forçado automático do MetroCluster".

Sobre esta tarefa

- Esta tarefa permite o switchover não planejado automático por padrão.
- Esta tarefa pode ser executada na interface ONTAP de qualquer nó na configuração IP do MetroCluster.

- Uma única instalação do serviço Mediador ONTAP pode ser configurada com até cinco configurações IP MetroCluster.

Passos

1. Adicione o serviço Mediador ONTAP ao ONTAP:

   `metrocluster configuration-settings mediator add -mediator-address` *`ip-address-of-mediator-host`*

   > Você será solicitado a fornecer o nome de usuário e a senha para a conta de usuário do administrador do Mediator.

2. Verifique se a funcionalidade de comutação automática está ativada:

   `metrocluster show`

3. Verifique se o Mediador está em execução.

   a. Mostrar os discos virtuais do Mediator:

      `storage disk show -container-type mediator`

      ```
       cluster_A::> storage disk show -container-type mediator
                               Usable           Disk    Container
      Container
       Disk                    Size Shelf Bay Type    Type        Name
      Owner
       ---------------- ---------- ----- --- ------- ----------- ---------
      --------
       NET-1.5                    -     -   - VMDISK  mediator    -
      node_A_2
       NET-1.6                    -     -   - VMDISK  mediator    -
      node_B_1
       NET-1.7                    -     -   - VMDISK  mediator    -
      node_B_2
       NET-1.8                    -     -   - VMDISK  mediator    -
      node_A_1
      ```

   b. Defina o modo de privilégio como avançado:

      `set advanced`

      ```
       cluster_A::> set advanced
      ```

   c. Exiba os iniciadores rotulados como mediador:

      `storage iscsi-initiator show -label mediator`

```
 cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
--------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

d. Verifique o estado do domínio de falha de switchover não planejado automático (AUSO):

`metrocluster show`

> A saída de exemplo a seguir se aplica ao ONTAP 9.13,1 e posterior. Para o ONTAP 9.12,1 e anteriores, o estado do domínio de falha do AUSO deve ser `auso-on-cluster-disaster`.

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-dr-group-disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-dr-group-disaster
```

4. Opcionalmente, configure o switchover forçado automático do MetroCluster.

Você só pode usar o seguinte comando em nível avançado de privilégio.

> Antes de utilizar este comando, reveja o "Riscos e limitações do uso do switchover forçado automático do MetroCluster".

`metrocluster modify -allow-auto-forced-switchover true`

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

Desconfigure o serviço do Mediador ONTAP a partir da configuração IP do MetroCluster

Você pode desconfigurar o serviço do Mediador ONTAP a partir da configuração IP do MetroCluster.

Antes de começar

Você deve ter instalado e configurado com êxito o Mediador ONTAP em um local de rede que possa ser acessado por ambos os sites MetroCluster.

Passos

1. Desconfigure o serviço do Mediador ONTAP usando o seguinte comando:

   `metrocluster configuration-settings mediator remove`

   Você será solicitado a fornecer o nome de usuário e a senha para a conta de usuário do administrador do ONTAP Mediator.

   > Se o Mediador do ONTAP estiver inativo, o `metrocluster configuration-settings mediator remove` comando ainda solicitará que você insira o nome de usuário e a senha da conta de usuário admin do ONTAP Mediator e removerá o serviço Mediador do ONTAP da configuração do MetroCluster.

   a. Verifique se há discos quebrados usando o seguinte comando:

      `disk show -broken`

      Exemplo

```
There are no entries matching your query.
```

2. Confirme se o serviço do Mediador ONTAP foi removido da configuração do MetroCluster executando os seguintes comandos em ambos os clusters:

   a. `metrocluster configuration-settings mediator show`

      Exemplo

```
This table is currently empty.
```

   b. `storage iscsi-initiator show -label mediator`

      Exemplo

```
There are no entries matching your query.
```

Conetando uma configuração do MetroCluster a uma instância diferente do ONTAP Mediator

Se você quiser conetar os nós do MetroCluster a uma instância diferente do Mediador do ONTAP, você deve desconfigurar e reconfigurar a conexão do Mediador no software ONTAP.

Antes de começar

Você precisa do nome de usuário, senha e endereço IP da nova instância do ONTAP Mediator.

Sobre esta tarefa

Esses comandos podem ser emitidos a partir de qualquer nó na configuração do MetroCluster.

Passos

1. Remova o Mediador ONTAP atual da configuração do MetroCluster:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Estabeleça a nova ligação do Mediador ONTAP à configuração do MetroCluster:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

Como o Mediador ONTAP suporta o switchover não planejado automático

O Mediador do ONTAP fornece LUNs de caixa de correio para armazenar informações de estado sobre os nós IP do MetroCluster. Esses LUNs são co-localizados com o Mediador ONTAP, que é executado em um host Linux fisicamente separado dos sites do MetroCluster. Os nós IP do MetroCluster podem usar as informações da caixa de correio para monitorar o estado de seus parceiros de recuperação de desastres (DR) e implementar um switchover não planejado assistido por mediador (MAUSO) em caso de desastre.

ⓘ O MAUSO não é compatível com configurações MetroCluster FC.

Quando um nó deteta uma falha do local que exige um switchover, ele toma medidas para confirmar que o switchover é apropriado e, em caso afirmativo, realiza o switchover. Por padrão, um MAUSO é iniciado para os seguintes cenários:

- O espelhamento do SyncMirror e o espelhamento de DR do cache não volátil de cada nó estão operando e os caches e espelhos são sincronizados no momento da falha.
- Nenhum dos nós no local sobrevivente está no estado de aquisição.
- Se ocorrer um desastre no local. Um desastre no local é uma falha de *todos* nós no mesmo local.

Um MAUSO é *not* iniciado nos seguintes cenários de desligamento:

- Inicia um encerramento. Por exemplo, quando você:
  - Parar os nós
  - Reinicie os nós

Saiba mais sobre os recursos do MAUSO disponíveis em cada versão do ONTAP 9.

Começando com…	Descrição
ONTAP 9.13,1	• Um MAUSO é iniciado se ocorrer um cenário predefinidoe uma falha de ventilador ou hardware inicia um desligamento ambiental. Exemplos de falhas de hardware incluem uma temperatura alta ou baixa, ou uma unidade de fonte de alimentação, bateria NVRAM ou falha de batimento cardíaco do processador de serviço. • O valor padrão para o domínio de falha é definido como "auso-on-dr-group" em uma configuração IP do MetroCluster. Para ONTAP 9.12,1 e anterior, o valor padrão é definido como "auso-on-cluster-disaster". Em uma configuração IP MetroCluster de oito nós, o "Auso-on-dr-group" aciona um MAUSO em caso de falha do cluster ou de um par de HA em um grupo de DR. Para um par de HA, ambos os nós precisam falhar ao mesmo tempo. Opcionalmente, você pode alterar a configuração de domínio de falha para o domínio "auso-on-cluster-disaster" usando o `metrocluster modify -auto-switchover -failure-domain auso-on-cluster-disaster` comando para acionar um MAUSO somente se houver falhas de par de nós de HA em ambos os grupos de DR. • Você pode alterar o comportamento para forçar um MAUSO mesmo que o NVRAM não esteja sincronizado no momento da falha.
ONTAP 9.12,1	Você pode ativar o recurso de switchover forçado automático do MetroCluster em uma configuração IP do MetroCluster usando o `metrocluster modify -allow-auto -forced-switchover true` comando. O switchover após a deteção de uma falha no local acontece automaticamente quando você ativa o recurso de switchover forçado automático do MetroCluster. Você pode usar esse recurso para complementar a funcionalidade de switchover automático MetroCluster IP. **Riscos e limitações do uso do switchover forçado automático do MetroCluster** Quando você permite que uma configuração IP do MetroCluster funcione no modo de comutação forçada automática, o seguinte problema conhecido pode levar à perda de dados: • A memória não volátil nas controladoras de storage não é espelhada para o parceiro de DR remoto no local do parceiro. **Atenção**: Você pode encontrar cenários que não são mencionados. A NetApp não é responsável por qualquer corrupção de dados, perda de dados ou outros danos que possam surgir ao ativar o recurso de switchover forçado automático do MetroCluster. Não utilize a funcionalidade de comutação forçada automática do MetroCluster se os riscos e limitações não forem aceitáveis para si.

Gerencie o Mediador ONTAP com o Gerenciador de sistemas

Usando o Gerenciador do sistema, você pode executar tarefas para gerenciar o Mediador do ONTAP.

Sobre estas tarefas

A partir do ONTAP 9.8, você pode usar o Gerenciador de sistema como uma interface simplificada para gerenciar uma configuração IP MetroCluster de quatro nós, que pode incluir um Mediador ONTAP instalado em um terceiro local.

A partir do ONTAP 9.14,1, você pode usar o Gerenciador do sistema para executar essas operações para um site IP MetroCluster de oito nós. Embora não seja possível configurar ou expandir um sistema de oito nós com o Gerenciador de sistema, se você já configurou um sistema IP MetroCluster de oito nós, então você pode executar essas operações.

Execute as seguintes tarefas para gerenciar o Mediador ONTAP.

Para executar esta tarefa…	Tome essas ações…
Configure o serviço Mediator	Ambos os clusters nos locais do MetroCluster devem estar ativos e colocados em Contato. **Passos** 1. No Gerenciador do sistema no ONTAP 9.8, selecione **Cluster > Configurações**. 2. Na seção **Mediator**, clique no ⚙. 3. Na janela **Configure Mediator**, clique em **Add**. 4. Introduza os detalhes de configuração do Mediador ONTAP. Você pode inserir os seguintes detalhes ao configurar um Mediador ONTAP com o Gerenciador de sistema. ◦ O endereço IP do Mediador. ◦ O nome de utilizador. ◦ A palavra-passe.

Ativar ou desativar o switchover automático assistido por Mediator (MAUSO)	**Passos** 1. No System Manager, clique em **Dashboard**. 2. Role até a seção MetroCluster. 3. Clique ⋮ ao lado do nome do site do MetroCluster. 4. Selecione **Enable** (Ativar) ou **Disable** (Desativar). 5. Introduza o nome de utilizador e a palavra-passe do administrador e, em seguida, clique em **Enable** (Ativar) ou **Disable** (Desativar). ⓘ Você pode ativar ou desativar o Mediador quando ele pode ser alcançado e ambos os sites estão no modo "normal". O Mediador ainda está acessível quando o MAUSO está ativado ou desativado se o sistema MetroCluster estiver em bom estado.
Remova o Mediador da configuração do MetroCluster	**Passos** 1. No System Manager, clique em **Dashboard**. 2. Role até a seção MetroCluster. 3. Clique ⋮ ao lado do nome do site do MetroCluster. 4. Selecione **Remover Mediador**. 5. Introduza o nome de utilizador e a palavra-passe do administrador e, em seguida, clique em **Remover**.
Verifique o estado do Mediador	Execute as etapas específicas do System Manager em "Verifique a integridade de uma configuração do MetroCluster".
Execute um switchover e um switchback	Execute as etapas em "Use o Gerenciador do sistema para executar o switchover e o switchback (somente configurações MetroCluster IP)".

Testando a configuração do MetroCluster

Você pode testar cenários de falha para confirmar o funcionamento correto da configuração do MetroCluster.

Verificando o switchover negociado

Você pode testar a operação switchover negociado (planejada) para confirmar a disponibilidade de dados ininterrupta.

Sobre esta tarefa

Este teste valida que a disponibilidade de dados não é afetada (exceto para os protocolos SMB (Server Message Block) da Microsoft e Fibre Channel do Solaris), alternando o cluster para o segundo data center.

Este teste deve levar cerca de 30 minutos.

Este procedimento tem os seguintes resultados esperados:

- O `metrocluster switchover` comando apresentará um prompt de aviso.

  Se você responder `yes` ao prompt, o site do qual o comando é emitido mudará para o site do parceiro.

Para configurações IP do MetroCluster:

- Para o ONTAP 9.4 e versões anteriores:
  - Os agregados espelhados ficarão degradados após o switchover negociado.
- Para o ONTAP 9.5 e posterior:
  - Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
  - Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Para o ONTAP 9.8 e posterior:
  - Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

Passos

1. Confirme se todos os nós estão no estado configurado e no modo normal:

   `metrocluster node show`

   ```
   cluster_A::>  metrocluster node show

   Cluster                           Configuration State    Mode
   --------------------------------- ----------------------
   -----------------------
    Local: cluster_A                  configured             normal
   Remote: cluster_B                  configured             normal
   ```

2. Inicie a operação de comutação:

   `metrocluster switchover`

   ```
   cluster_A::> metrocluster switchover
   Warning: negotiated switchover is about to start. It will stop all the
   data Vservers on cluster "cluster_B" and
   automatically re-start them on cluster "cluster_A". It will finally
   gracefully shutdown cluster "cluster_B".
   ```

3. Confirme se o cluster local está no estado configurado e no modo de comutação:

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. Confirme se a operação de comutação foi bem-sucedida:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Use os `vserver show` comandos e `network interface show` para verificar se as SVMs e LIFs de DR estão online.

Verificando a cura e a troca manual

Você pode testar as operações de reparo e switchback manual para verificar se a disponibilidade de dados não é afetada (exceto para configurações SMB e Solaris FC), alternando o cluster para o data center original após um switchover negociado.

Sobre esta tarefa

Este teste deve levar cerca de 30 minutos.

O resultado esperado deste procedimento é que os serviços devem ser reenviados para os seus nós domésticos.

Os passos de recuperação não são necessários em sistemas que executam o ONTAP 9.5 ou posterior, nos quais a recuperação é realizada automaticamente após um switchover negociado. Em sistemas que executam o ONTAP 9.6 e posterior, a recuperação também é executada automaticamente após o switchover não programado.

Passos

1. Se o sistema estiver executando o ONTAP 9.4 ou anterior, corrija o agregado de dados:

   `metrocluster heal aggregates`

   O exemplo a seguir mostra a conclusão bem-sucedida do comando:

```
cluster_A::> metrocluster heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. Se o sistema estiver executando o ONTAP 9.4 ou anterior, sane o agregado raiz:

   `metrocluster heal root-aggregates`

   Esta etapa é necessária nas seguintes configurações:

   - Configurações de FC MetroCluster.
   - Configurações IP do MetroCluster executando o ONTAP 9.4 ou anterior. O exemplo a seguir mostra a conclusão bem-sucedida do comando:

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. Verifique se a cicatrização está concluída:

   `metrocluster node show`

   O exemplo a seguir mostra a conclusão bem-sucedida do comando:

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   heal roots
completed
      cluster_B
              node_B_2         unreachable    -         switched over
42 entries were displayed.metrocluster operation show
```

   Se a operação de recuperação automática falhar por qualquer motivo, você deve emitir os `metrocluster heal` comandos manualmente, como feito nas versões do ONTAP anteriores ao ONTAP 9.5. Você pode usar os `metrocluster operation show` comandos e `metrocluster operation history show -instance` para monitorar o status da recuperação e determinar a causa de uma falha.

4. Verifique se todos os agregados estão espelhados:

   `storage aggregate show`

   O exemplo a seguir mostra que todos os agregados têm um status RAID espelhado:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

5. Verifique o status da recuperação de switchback:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
             node_A_1           configured     enabled   heal roots
completed
      cluster_B
             node_B_2           configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

6. Execute o interrutor de retorno:

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

7. Confirme o status dos nós:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   normal
      cluster_B
              node_B_2         configured     enabled   normal

2 entries were displayed.
```

8. Confirmar o estado da operação MetroCluster:

```
metrocluster operation show
```

A saída deve mostrar um estado bem-sucedido.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Verificação da operação após interrupção da linha elétrica

Você pode testar a resposta da configuração do MetroCluster à falha de uma PDU.

Sobre esta tarefa

A prática recomendada é que cada unidade de fonte de alimentação (PSU) de um componente seja conetada a fontes de alimentação separadas. Se ambas as PSUs estiverem conetadas à mesma unidade de distribuição de energia (PDU) e ocorrer uma interrupção elétrica, o local pode ficar inativo ou um compartimento completo pode ficar indisponível. A falha de uma linha de alimentação é testada para confirmar que não há incompatibilidade de cabeamento que possa causar uma interrupção do serviço.

Este teste deve levar cerca de 15 minutos.

Este teste requer a desativação da energia de todas as PDUs do lado esquerdo e, em seguida, de todas as PDUs do lado direito em todos os racks que contêm os componentes do MetroCluster.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados à medida que as PDUs são desconetadas.
- Nenhum failover ou perda de serviço deve ocorrer.

Passos

1. Desligue a alimentação das PDUs no lado esquerdo do rack que contém os componentes MetroCluster.
2. Monitore o resultado no console:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

   ```
   cluster_A::> system environment sensors show -state fault

   Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
   Crit-Hi
   ---- -------------------- ------ ----------- -------- -------- -------
   -------
   node_A_1
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   node_A_2
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   4 entries were displayed.

   cluster_A::> storage shelf show -errors
       Shelf Name: 1.1
        Shelf UID: 50:0a:09:80:03:6c:44:d5
    Serial Number: SHFHU1443000059

   Error Type          Description
   ------------------  --------------------------
   Power               Critical condition is detected in storage shelf
   power supply unit "1". The unit might fail.Reconnect PSU1
   ```

3. Ligue a alimentação novamente para as PDUs do lado esquerdo.

4. Certifique-se de que o ONTAP limpa a condição de erro.
5. Repita os passos anteriores com as PDUs do lado direito.

Verificação da operação após a perda de uma única prateleira de armazenamento

Você pode testar a falha de um único compartimento de storage para verificar se não há um ponto único de falha.

Sobre esta tarefa

Este procedimento tem os seguintes resultados esperados:

- Uma mensagem de erro deve ser comunicada pelo software de monitorização.
- Nenhum failover ou perda de serviço deve ocorrer.
- A ressincronização do espelho é iniciada automaticamente após a restauração da falha de hardware.

Passos

1. Verifique o status de failover de armazenamento:

   `storage failover show`

   ```
   cluster_A::> storage failover show

   Node           Partner        Possible State Description
   -------------- -------------- --------
   -------------------------------------
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Verifique o status agregado:

   `storage aggregate show`

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Verifique se todas as SVMs e volumes de dados estão on-line e fornecendo dados:

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identifique um compartimento no pool 1 para o nó "node_A_2" para desligar para simular uma falha repentina de hardware:

`storage aggregate show -r -node node-name !*root`

O compartimento selecionado deve conter unidades que fazem parte de um agregado de dados espelhados.

No exemplo a seguir, o ID do compartimento "31" é selecionado para falhar.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                     1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                     1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.3                     1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                     1   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     1.31.5                          1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                     0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Desligue fisicamente a prateleira selecionada.
6. Verifique novamente o status do agregado:

```
storage aggregate show

storage aggregate show -r -node node_A_2 !*root
```

O agregado com unidades no compartimento desligado deve ter um status RAID "degradado" e as unidades no Plex afetado devem ter um status de "falha", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,
```

```
mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.6                          0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                          0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                          0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                      -   -          -  827.7GB
-  (failed)
     parity   FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)
     data     FAILED                      -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Verifique se os dados estão sendo fornecidos e se todos os volumes ainda estão online:

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Ligue fisicamente a prateleira.

   A ressincronização é iniciada automaticamente.

9. Verifique se a ressincronização foi iniciada:

   `storage aggregate show`

   O agregado afetado deve ter um status RAID de "ressincronização", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. Monitore o agregado para confirmar que a ressincronização está concluída:

    `storage aggregate show`

    O agregado afetado deve ter um status RAID "normal", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Considerações ao remover configurações do MetroCluster

Depois de remover a configuração do MetroCluster, toda a conetividade de disco e interconexões devem ser ajustadas para estar em um estado suportado. Se precisar remover a configuração do MetroCluster, entre em Contato com o suporte técnico.

Não é possível reverter a desconfiguração do MetroCluster. Este processo só deve ser feito com a assistência de suporte técnico. Entre em Contato com o suporte técnico da NetApp e consulte o guia apropriado para sua configuração no "Como remover nós de uma configuração MetroCluster - Guia de resolução."

Considerações ao usar o ONTAP em uma configuração do MetroCluster

Ao usar o ONTAP em uma configuração do MetroCluster, você deve estar ciente de certas considerações sobre licenciamento, peering para clusters fora da configuração do MetroCluster, execução de operações de volume, operações NVFAIL e outras operações do ONTAP.

A configuração do ONTAP dos dois clusters, incluindo a rede, deve ser idêntica, porque o recurso MetroCluster depende da capacidade de um cluster de servir dados de forma otimizada para seu parceiro no caso de um switchover.

Considerações sobre licenciamento

- Ambos os sites devem ser licenciados para os mesmos recursos licenciados pelo site.
- Todos os nós devem ser licenciados para os mesmos recursos de bloqueio de nó.

Consideração de SnapMirror

- A recuperação de desastres do SnapMirror SVM só é compatível com configurações do MetroCluster executando versões do ONTAP 9.5 ou posterior.

Operações do MetroCluster no Gerenciador de sistemas do ONTAP

Dependendo da versão do ONTAP, algumas operações específicas do MetroCluster podem ser executadas usando o Gerenciador de sistemas do ONTAP.

Para saber mais, consulte "Gerencie sites do MetroCluster com o Gerenciador de sistemas"a documentação.

Suporte FlexCache em uma configuração MetroCluster

A partir do ONTAP 9.7, os volumes FlexCache são compatíveis com configurações do MetroCluster. Você deve estar ciente dos requisitos para a repetibilidade manual após operações de comutação ou switchback.

Repetibilidade da SVM após o switchover quando a origem e o cache do FlexCache estão no mesmo local do MetroCluster

Após um switchover negociado ou não planejado, qualquer relacionamento de peering SVM FlexCache no cluster deve ser configurado manualmente.

Por exemplo, svms VS1 (cache) e VS2 (origem) estão no site_A. Esses SVMs são peered.

Após o switchover, os svms VS1-MC e VS2-mc são ativados no local do parceiro (site_B). Eles devem ser repelidos manualmente para que o FlexCache funcione usando o comando vserver peer repeer.

Repetibilidade da SVM após switchover ou switchback quando um destino FlexCache está em um terceiro cluster e no modo desconetado

Para relacionamentos do FlexCache com um cluster fora da configuração do MetroCluster, o peering deve ser sempre reconfigurado manualmente após um switchover, se os clusters envolvidos estiverem no modo desconetado durante o switchover.

Por exemplo:

- Um fim do FlexCache (cache_1 no VS1) reside no MetroCluster site_A tem um fim do FlexCache
- A outra extremidade do FlexCache (origin_1 no VS2) reside no site_C (não na configuração do MetroCluster)

Quando o switchover é acionado, e se o site_A e o site_C não estiverem conetados, você deve repelir manualmente os SVMs no site_B (o cluster de switchover) e site_C usando o comando vserver peer repetier após o switchover.

Quando o switchback é executado, você deve repelir novamente os SVMs no site_A (o cluster original) e site_C.

Informações relacionadas

"Gerenciamento de volumes do FlexCache com a CLI"

Suporte FabricPool em configurações MetroCluster

A partir do ONTAP 9.7, as configurações do MetroCluster são compatíveis com camadas de storage FabricPool.

Para obter informações gerais sobre como usar o FabricPools, "Gerenciamento de disco e camada (agregado)" consulte .

Considerações ao usar FabricPools

- Os clusters precisam ter licenças FabricPool com limites de capacidade correspondentes.
- Os clusters devem ter IPspaces com nomes correspondentes.

  Esse pode ser o espaço IPspace padrão ou um espaço IP criado por um administrador. Este espaço IPspace será usado para configurações de armazenamento de objetos FabricPool.

- Para o espaço IPspace selecionado, cada cluster deve ter um LIF entre clusters definido que possa alcançar o armazenamento de objetos externo

Configurando um agregado para uso em um FabricPool espelhado

Antes de configurar o agregado, você deve configurar armazenamentos de objetos conforme descrito em "Configurando armazenamentos de objetos para FabricPool em uma configuração MetroCluster" em "Gerenciamento de disco e agregado".

Passos

Para configurar um agregado para uso em um FabricPool:

1. Crie o agregado ou selecione um agregado existente.

2. Espelhe o agregado como um agregado espelhado típico na configuração do MetroCluster.
3. Crie o espelho FabricPool com o agregado, conforme descrito em "Gerenciamento de disco e agregado"
   a. Anexe um armazenamento de objetos primário.

      Este armazenamento de objetos está fisicamente mais perto do cluster.

   b. Adicione um armazenamento de objetos espelhados.

      Este armazenamento de objetos está fisicamente mais distante do cluster do que o armazenamento de objetos primário.

Suporte FlexGroup em configurações MetroCluster

A partir do ONTAP 9.6, as configurações do MetroCluster são compatíveis com volumes FlexGroup.

Programações de trabalhos em uma configuração MetroCluster

No ONTAP 9.3 e posterior, as programações de tarefas criadas pelo usuário são replicadas automaticamente entre clusters em uma configuração do MetroCluster. Se você criar, modificar ou excluir um agendamento de trabalho em um cluster, o mesmo agendamento será criado automaticamente no cluster de parceiros, usando o CRS (Configuration Replication Service).

As programações criadas pelo sistema não são replicadas e você deve executar manualmente a mesma operação no cluster de parceiros para que as programações de tarefas em ambos os clusters sejam idênticas.

Peering de cluster do site MetroCluster para um terceiro cluster

Como a configuração de peering não é replicada, se você identificar um dos clusters na configuração do MetroCluster para um terceiro cluster fora dessa configuração, você também deverá configurar o peering no cluster do MetroCluster parceiro. Isso é para que o peering possa ser mantido se ocorrer um switchover.

O cluster que não é MetroCluster deve estar executando o ONTAP 8,3 ou posterior. Caso contrário, o peering é perdido se ocorrer um switchover, mesmo que o peering tenha sido configurado em ambos os parceiros da MetroCluster.

Replicação de configuração de cliente LDAP em uma configuração MetroCluster

Uma configuração de cliente LDAP criada em uma máquina virtual de storage (SVM) em um cluster local é replicada para os dados de parceiros SVM no cluster remoto. Por exemplo, se a configuração do cliente LDAP for criada no SVM admin no cluster local, ela será replicada para todos os SVMs de dados administrativos no cluster remoto. Esse recurso do MetroCluster é intencional para que a configuração do cliente LDAP esteja ativa em todos os SVMs de parceiros no cluster remoto.

Diretrizes de criação de LIF e rede para configurações do MetroCluster

Você deve estar ciente de como LIFs são criados e replicados em uma configuração do MetroCluster. Você também deve saber sobre o requisito de consistência para que você possa tomar as decisões adequadas ao configurar sua rede.

Informações relacionadas

"Gerenciamento de rede e LIF"

"Requisitos de replicação de objeto IPspace e configuração de sub-rede"

"Requisitos para criação de LIF em uma configuração MetroCluster"

"Requisitos e problemas de replicação e posicionamento de LIF"

Requisitos de replicação de objeto IPspace e configuração de sub-rede

Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

Replicação IPspace

Você deve considerar as diretrizes a seguir enquanto replica objetos IPspace para o cluster de parceiros:

- Os nomes de IPspace dos dois locais devem corresponder.
- Os objetos IPspace devem ser replicados manualmente para o cluster do parceiro.

  Quaisquer máquinas virtuais de armazenamento (SVMs) que sejam criadas e atribuídas a um IPspace antes que o IPspace seja replicado não serão replicadas para o cluster de parceiros.

Configuração de sub-rede

Você deve considerar as seguintes diretrizes ao configurar sub-redes em uma configuração do MetroCluster:

- Ambos os clusters da configuração do MetroCluster devem ter uma sub-rede no mesmo espaço IPspace com o mesmo nome de sub-rede, sub-rede, domínio de broadcast e gateway.
- Os intervalos de IP dos dois clusters devem ser diferentes.

  No exemplo a seguir, os intervalos de IP são diferentes:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------       -------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      --------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.21-192.168.2.30
```

Configuração IPv6

Se o IPv6 estiver configurado em um site, o IPv6 também deve ser configurado no outro site.

Informações relacionadas

"Requisitos para criação de LIF em uma configuração MetroCluster"

"Requisitos e problemas de replicação e posicionamento de LIF"

Requisitos para criação de LIF em uma configuração MetroCluster

Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

Você deve considerar as seguintes diretrizes ao criar LIFs:

- Fibre Channel: Você precisa usar VSAN esticada ou tecidos esticados
- IP/iSCSI: Você deve usar a rede estendida da camada 2
- Broadcasts ARP: Você deve habilitar broadcasts ARP entre os dois clusters
- LIFs duplicadas: Você não deve criar vários LIFs com o mesmo endereço IP (LIFs duplicadas) em um espaço IPspace
- Configurações NFS e SAN: Você precisa usar diferentes máquinas virtuais de storage (SVMs) para agregados sem espelhamento e espelhados
- Você deve criar um objeto de sub-rede antes de criar um LIF. Um objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque tem um domínio de broadcast associado.

Verifique a criação de LIF

Você pode confirmar a criação bem-sucedida de um LIF em uma configuração MetroCluster executando o comando MetroCluster check lif show. Se você encontrar algum problema ao criar o LIF, você pode usar o comando MetroCluster check lif repair-placement para corrigir os problemas.

Informações relacionadas

"Requisitos de replicação de objeto IPspace e configuração de sub-rede"

"Requisitos e problemas de replicação e posicionamento de LIF"

Requisitos e problemas de replicação e posicionamento de LIF

Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

Replicação de LIFs para o cluster de parceiros

Quando você cria um LIF em um cluster em uma configuração do MetroCluster, o LIF é replicado no cluster de parceiros. LIFs não são colocados em uma base de nome individual. Para disponibilidade de LIFs após uma operação de switchover, o processo de colocação de LIF verifica se as portas são capazes de hospedar o LIF com base em verificações de acessibilidade e atributos de porta.

O sistema deve atender às seguintes condições para colocar as LIFs replicadas no cluster de parceiros:

Condição	Tipo de LIF: FC	Tipo de LIF: IP/iSCSI
Identificação do nó	O ONTAP tenta colocar o LIF replicado no parceiro de recuperação de desastres (DR) do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.	O ONTAP tenta colocar o LIF replicado no parceiro de DR do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.
Identificação da porta	O ONTAP identifica as portas de destino FC conectadas no cluster de DR.	As portas no cluster de DR que estão no mesmo IPspace que o LIF de origem são selecionadas para uma verificação de acessibilidade.se não houver portas no cluster de DR no mesmo IPspace, o LIF não pode ser colocado. Todas as portas no cluster de DR que já estão hospedando um LIF no mesmo espaço IPspace e sub-rede são marcadas automaticamente como alcançáveis e podem ser usadas para o posicionamento. Essas portas não estão incluídas na verificação de acessibilidade.

Verificação de acessibilidade	A acessibilidade é determinada verificando a conetividade da malha de origem WWN nas portas do cluster de DR. Se a mesma malha não estiver presente no local de DR, o LIF é colocado em uma porta aleatória no parceiro de DR.	A acessibilidade é determinada pela resposta a um broadcast ARP (Address Resolution Protocol) de cada porta identificada anteriormente no cluster DR para o endereço IP de origem do LIF a ser colocado.para que as verificações de acessibilidade tenham êxito, as emissões ARP devem ser permitidas entre os dois clusters. Cada porta que recebe uma resposta do LIF de origem será marcada como possível para o posicionamento.
Seleção da porta	O ONTAP categoriza as portas com base em atributos como tipo e velocidade do adaptador e, em seguida, seleciona as portas com atributos correspondentes.se não forem encontradas portas com atributos correspondentes, o LIF é colocado em uma porta conetada aleatória no parceiro DR.	A partir das portas marcadas como alcançáveis durante a verificação de acessibilidade, o ONTAP prefere as portas que estão no domínio de broadcast associado à sub-rede do LIF. Se não houver portas de rede disponíveis no cluster de DR que estão no domínio de broadcast associado à sub-rede do LIF, o ONTAP seleciona as portas que têm acessibilidade para o LIF de origem. Se não houver portas com acessibilidade ao LIF de origem, uma porta será selecionada do domínio de broadcast associado à sub-rede do LIF de origem e, se nenhum domínio de broadcast existir, uma porta aleatória será selecionada. O ONTAP categoriza as portas com base em atributos como tipo de adaptador, tipo de interface e velocidade e, em seguida, seleciona as portas com atributos correspondentes.
Colocação de LIF	A partir das portas alcançáveis, o ONTAP seleciona a porta menos carregada para colocação.	A partir das portas selecionadas, o ONTAP seleciona a porta menos carregada para colocação.

Colocação de LIFs replicadas quando o nó do parceiro de DR está inativo

Quando um iSCSI ou FC LIF é criado em um nó cujo parceiro de DR foi assumido, o LIF replicado é colocado no nó do parceiro auxiliar de DR. Após uma operação subsequente de giveback, os LIFs não são movidos automaticamente para o parceiro DR. Isso pode levar a que os LIFs se concentrem em um único nó no cluster de parceiros. Durante uma operação de switchover do MetroCluster, tentativas subsequentes de mapear LUNs pertencentes à máquina virtual de storage (SVM) falham.

Você deve executar o `metrocluster check lif show` comando após uma operação de aquisição ou operação de giveback para verificar se o posicionamento de LIF está correto. Se existirem erros, pode executar o `metrocluster check lif repair-placement` comando para resolver os problemas.

Erros de colocação de LIF

Os erros de colocação de LIF que são exibidos pelo `metrocluster check lif show` comando são retidos após uma operação de comutação. Se o `network interface modify` comando , `network interface rename` ou `network interface delete` for emitido para um LIF com um erro de posicionamento, o erro será removido e não aparecerá na saída do `metrocluster check lif show` comando.

Falha de replicação de LIF

Você também pode verificar se a replicação do LIF foi bem-sucedida usando o `metrocluster check lif show` comando. Uma mensagem EMS é exibida se a replicação LIF falhar.

Você pode corrigir uma falha de replicação executando o `metrocluster check lif repair-placement` comando para qualquer LIF que não consiga encontrar uma porta correta. Você deve resolver quaisquer falhas de replicação de LIF o mais rápido possível para verificar a disponibilidade de LIF durante uma operação de switchover de MetroCluster.

> Mesmo que o SVM de origem esteja inativo, o posicionamento de LIF pode continuar normalmente se houver um LIF pertencente a um SVM diferente em uma porta com o mesmo espaço IPspace e rede no SVM de destino.

Informações relacionadas

"Requisitos de replicação de objeto IPspace e configuração de sub-rede"

"Requisitos para criação de LIF em uma configuração MetroCluster"

Criação de volume em um agregado raiz

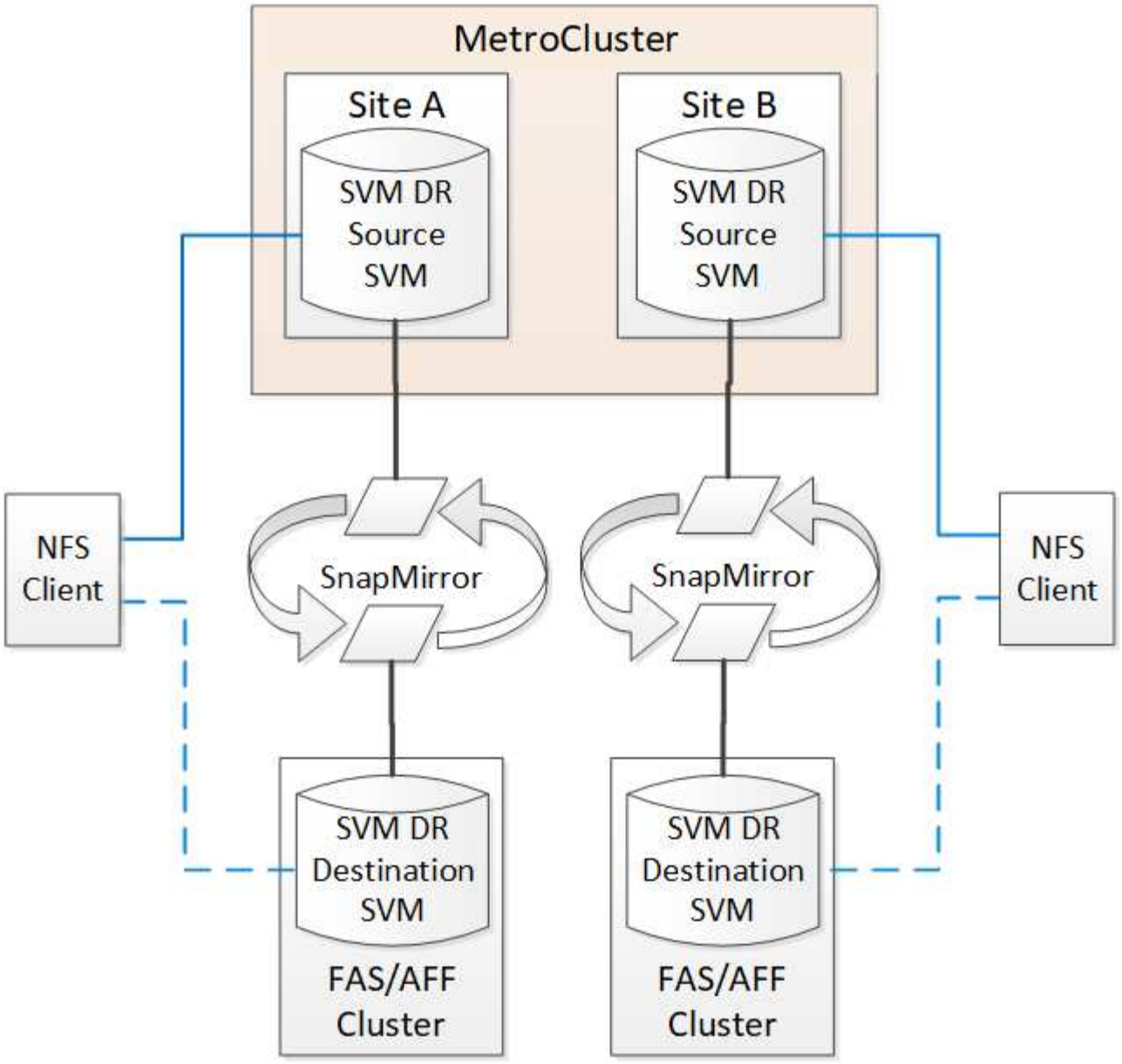
O sistema não permite a criação de novos volumes no agregado raiz (um agregado com uma política de HA do CFO) de um nó em uma configuração do MetroCluster.

Devido a essa restrição, os agregados de raiz não podem ser adicionados a um SVM usando o `vserver add-aggregates` comando.

Recuperação de desastres do SVM em uma configuração de MetroCluster

A partir do ONTAP 9.5, as máquinas virtuais de storage ativo (SVMs) em uma configuração do MetroCluster podem ser usadas como fontes com o recurso de recuperação de desastres do SnapMirror SVM. O SVM de destino deve estar no terceiro cluster fora da configuração do MetroCluster.

A partir do ONTAP 9.11,1, ambos os locais em uma configuração do MetroCluster podem ser a origem de uma relação de SVM DR com um cluster de destino FAS ou AFF, conforme mostrado na imagem a seguir.



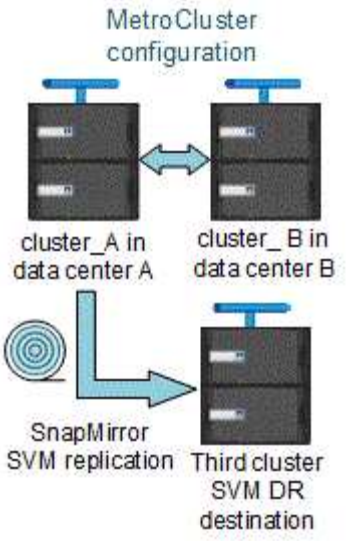
Você deve estar ciente dos seguintes requisitos e limitações de uso de SVMs com recuperação de desastres do SnapMirror:

- Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM.

  Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover.

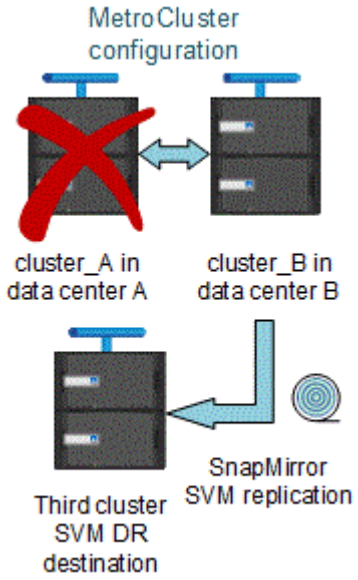
- Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online.

  A imagem a seguir mostra o comportamento de recuperação de desastres do SVM em um estado estável:



- Quando o SVM de origem sincronizada é a fonte de uma relação SVM DR, as informações de origem no relacionamento de SVM DR são replicadas para o parceiro MetroCluster.

  Isso permite que as atualizações do SVM DR continuem após um switchover, conforme mostrado na imagem a seguir:



- Durante os processos de switchover e switchback, a replicação para o destino SVM DR pode falhar.

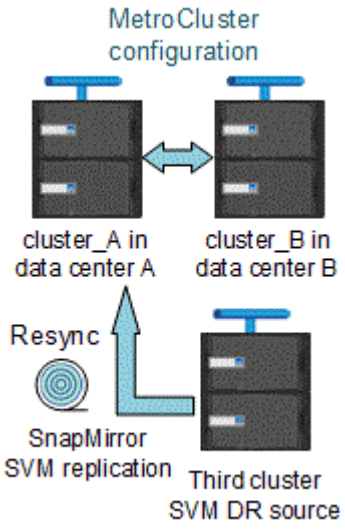
  No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas do SVM DR serão bem-sucedidas.

Consulte ""replicando a configuração do SVM"" em "Proteção de dados" para obter detalhes sobre como configurar uma relação de SVM DR.

Ressincronização da SVM em um local de recuperação de desastre

Durante a ressincronização, a fonte de recuperação de desastres (DR) de máquinas virtuais de storage (SVMs) na configuração MetroCluster é restaurada a partir do SVM de destino no local que não é MetroCluster.

Durante a ressincronização, o SVM de origem (cluster_A) atua temporariamente como SVM de destino, conforme mostrado na imagem a seguir:



Se um switchover não planejado ocorrer durante a ressincronização

Switchovers não planejados que ocorrem durante a ressincronização interromperão a transferência de ressincronização. Se ocorrer um switchover não planejado, as seguintes condições são verdadeiras:

- O SVM de destino no local do MetroCluster (que era uma fonte SVM antes da ressincronização) permanece como um SVM de destino. O SVM no cluster de parceiros continuará mantendo seu subtipo e inativo.
- A relação do SnapMirror deve ser recriada manualmente com o SVM de destino de sincronização como destino.
- A relação SnapMirror não aparece na saída do show do SnapMirror após um switchover no local sobrevivente, a menos que uma operação de criação do SnapMirror seja executada.

Execução do switchback após um switchover não planejado durante a ressincronização

Para executar com sucesso o processo de switchback, a relação de ressincronização deve ser quebrada e excluída. O switchback não é permitido se houver algum SVMs de destino de DR do SnapMirror na configuração do MetroCluster ou se o cluster tiver um SVM de subtipo "dp-destination".

A saída para o comando storage Aggregate plex show é indeterminada após um switchover do MetroCluster

Quando você executa o comando storage Aggregate plex show após um switchover do MetroCluster, o status de plex0 do agregado de raiz comutada é indeterminado e é exibido como falhou. Durante este tempo, a raiz comutada não é atualizada. O estado real deste Plex só pode ser determinado após a fase de cicatrização do MetroCluster.

Modificação de volumes para definir o sinalizador NVFAIL em caso de comutação

Você pode modificar um volume para que o sinalizador NVFAIL seja definido no volume em caso de um switchover MetroCluster. O sinalizador NVFAIL faz com que o volume seja vedado de qualquer modificação. Isso é necessário para volumes que precisam ser tratados como se as gravações confirmadas no volume fossem perdidas após o switchover.

Nas versões do ONTAP anteriores a 9,0, o sinalizador NVFAIL é usado para cada switchover. No ONTAP 9.0 e versões posteriores, o switchover não planejado (USO) é usado.

Passo

1. Ative a configuração do MetroCluster para ativar o NVFAIL no switchover definindo o `vol -dr-force -nvfail` parâmetro como On:

```
vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
```

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster"	• Compreender a configuração do MetroCluster • Switchover, cura e switchback
"Recuperação de desastres"	• Recuperação de desastres • Comutação forçada • Recuperação de uma falha de vários controladores ou armazenamento

"Manutenção MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster FC • Procedimentos de substituição ou atualização de hardware e atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conetada à malha • Substituição de hardware em um local de desastre em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.
"Atualização e expansão do MetroCluster"	• Atualizando ou atualizando uma configuração do MetroCluster • Expansão de uma configuração do MetroCluster com a adição de nós adicionais
"Transição do MetroCluster"	• Transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP
"Atualização, transição e expansão do MetroCluster"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
"Documentação dos sistemas de hardware da ONTAP" **Nota:** os procedimentos de manutenção de prateleira de armazenamento padrão podem ser usados com configurações MetroCluster IP.	• Adição automática de um compartimento de disco • Remoção automática de um compartimento de disco
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
"Conceitos de ONTAP"	• Como os agregados espelhados funcionam

Instale uma configuração Stretch MetroCluster

Visão geral

Para instalar sua configuração Stretch MetroCluster, você deve executar vários procedimentos na ordem correta.

- "Prepare-se para a instalação e entenda todos os requisitos"
- "Escolha o procedimento de instalação correto"
- Faça o cabo dos componentes
  - "Configuração de conexão SAS de dois nós"
  - "Configuração de conexão em ponte de dois nós"
- "Configure o software"
- "Teste a configuração"

Prepare-se para a instalação do MetroCluster

Diferenças entre as configurações do ONTAP MetroCluster

As várias configurações do MetroCluster têm diferenças importantes nos componentes necessários.

Em todas as configurações, cada um dos dois locais do MetroCluster é configurado como um cluster do ONTAP. Em uma configuração de MetroCluster de dois nós, cada nó é configurado como um cluster de nó único.

Recurso	Configurações IP	Configurações conectadas à malha		Configurações elásticas	
		Quatro ou oito nós	* Dois nós*	* Dois nós bridge-attached*	**Conexão direta de dois nós**
Número de controladores	Quatro ou oito*	Quatro ou oito	Dois	Dois	Dois
Usa uma malha de storage de switch FC	Não	Sim	Sim	Não	Não
Usa uma malha de storage de switch IP	Sim	Não	Não	Não	Não
Usa pontes FC para SAS	Não	Sim	Sim	Sim	Não

Usa o storage SAS com conexão direta	Sim (apenas anexo local)	Não	Não	Não	Sim
Suporta ADP	Sim (começando com ONTAP 9.4)	Não	Não	Não	Não
Suporta HA local	Sim	Sim	Não	Não	Não
Compatível com o switchover não planejado automático do ONTAP (AUSO)	Não	Sim	Sim	Sim	Sim
Compatível com agregados sem espelhamento	Sim (começando com ONTAP 9.8)	Sim	Sim	Sim	Sim
Compatível com LUNs de array	Não	Sim	Sim	Sim	Sim
Suporta o Mediador ONTAP	Sim (começando com ONTAP 9.7)	Não	Não	Não	Não
Compatível com o tiebreaker MetroCluster	Sim (não em combinação com o Mediador ONTAP)	Sim	Sim	Sim	Sim
Suportes Todos os arrays SAN	Sim	Sim	Sim	Sim	Sim

Importante

Observe as seguintes considerações para configurações de IP MetroCluster de oito nós:

- As configurações de oito nós são suportadas a partir do ONTAP 9.9,1.
- Somente switches MetroCluster validados pela NetApp (solicitados pela NetApp) são compatíveis.
- Configurações que usam conexões de back-end roteadas por IP (camada 3) não são suportadas.
- As configurações que usam redes de camada privada compartilhada 2 não são suportadas.
- As configurações que usam um switch compartilhado Cisco 9336C-FX2 não são suportadas.

Suporte para todos os sistemas de storage SAN nas configurações do MetroCluster

Alguns dos All SAN Arrays (ASAs) são suportados nas configurações do MetroCluster. Na documentação do MetroCluster, as informações dos modelos AFF aplicam-se ao sistema ASA correspondente. Por exemplo, todo o cabeamento e outras informações do sistema AFF A400 também se aplicam ao sistema ASA AFF

A400.

As configurações de plataforma compatíveis estão listadas no "NetApp Hardware Universe".

Peering de clusters

Cada site do MetroCluster é configurado como um ponto do site do parceiro. Você deve estar familiarizado com os pré-requisitos e diretrizes para configurar as relações de peering. Isso é importante ao decidir se usar portas compartilhadas ou dedicadas para esses relacionamentos.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar que a conetividade entre os requisitos de porta, endereço IP, sub-rede, firewall e nomenclatura de cluster é atendida.

Requisitos de conetividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

  Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.

> O ONTAP 9 permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

  Você pode usar vários IPspaces para fazer pares com vários clusters. A conetividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

  As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Serviço ICMP
- TCP para os endereços IP de todos os LIFs entre clusters nas portas 10000, 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

A política de firewall entre clusters padrão permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Considerações ao usar portas dedicadas

Ao determinar se o uso de uma porta dedicada para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alteração e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o uso de uma porta dedicada é a melhor solução de rede entre clusters:

- Se a quantidade de largura de banda da WAN disponível for semelhante à das portas LAN e o intervalo de replicação for tal que a replicação ocorra enquanto a atividade do cliente regular existe, você deve dedicar portas Ethernet para replicação entre clusters para evitar a contenção entre replicação e os protocolos de dados.
- Se a utilização da rede gerada pelos protocolos de dados (CIFS, NFS e iSCSI) for tal que a utilização da rede seja superior a 50%, dedique portas para replicação para permitir desempenho não degradado se ocorrer um failover de nó.
- Quando portas físicas de 10 GbE ou mais rápidas são usadas para dados e replicação, você pode criar portas VLAN para replicação e dedicar as portas lógicas para replicação entre clusters.

  A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.

Considerações ao compartilhar portas de dados

Ao determinar se o compartilhamento de uma porta de dados para replicação entre clusters é a solução de rede entre clusters correta, você deve considerar configurações e requisitos, como tipo de LAN, largura de banda da WAN disponível, intervalo de replicação, taxa de alterações e número de portas.

Considere os seguintes aspetos da sua rede para determinar se o compartilhamento de portas de dados é a melhor solução de conetividade entre clusters:

- Para uma rede de alta velocidade, como uma rede 40-Gigabit Ethernet (40-GbE), uma quantidade suficiente de largura de banda local da LAN pode estar disponível para executar a replicação nas mesmas portas de 40 GbE que são usadas para acesso aos dados.

  Em muitos casos, a largura de banda da WAN disponível é muito menor do que a largura de banda da LAN de 10 GbE.

- Todos os nós no cluster podem ter que replicar dados e compartilhar a largura de banda da WAN disponível, tornando o compartilhamento da porta de dados mais aceitável.
- O compartilhamento de portas para dados e replicação elimina as contagens de portas extras necessárias para dedicar portas para replicação.
- O tamanho máximo da unidade de transmissão (MTU) da rede de replicação será o mesmo tamanho que o utilizado na rede de dados.
- Considere a taxa de alteração de dados e o intervalo de replicação e se a quantidade de dados, que deve ser replicada em cada intervalo, requer largura de banda suficiente. Isso pode causar contenção com protocolos de dados se compartilhar portas de dados.
- Quando as portas de dados para replicação entre clusters são compartilhadas, as LIFs entre clusters podem ser migradas para qualquer outra porta compatível com clusters no mesmo nó para controlar a porta de dados específica usada para replicação.

Considerações ao usar agregados sem espelhamento

Considerações ao usar agregados sem espelhamento

Se a sua configuração incluir agregados sem espelhamento, você precisa estar ciente de possíveis problemas de acesso que seguem as operações de switchover.

Considerações para agregados sem espelhamento ao fazer manutenção que requer desligamento de energia

Se você estiver executando um switchover negociado por motivos de manutenção que exigem desligamento de energia em todo o local, primeiro deverá ficar offline manualmente todos os agregados sem espelhamento pertencentes ao local de desastre.

Se você não colocar nenhum agregado sem espelhamento off-line, os nós no site sobrevivente podem ficar inativos devido a panics de vários discos. Isso pode ocorrer se agregados comutados por espelhamento ficarem off-line ou estiverem ausentes, devido à perda de conectividade com storage no local de desastre. Este é o resultado de um desligamento de energia ou uma perda de ISLs.

Considerações para agregados sem espelhamento e namespaces hierárquicos

Se você estiver usando namespaces hierárquicos, você deve configurar o caminho de junção para que todos os volumes nesse caminho estejam apenas em agregados espelhados ou apenas em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados no caminho de junção pode impedir o acesso aos agregados sem espelhamento após a operação de comutação.

Considerações para agregados sem espelhamento e volumes de metadados CRS e volumes raiz de dados SVM

O volume de metadados do serviço de replicação de configuração (CRS) e os volumes raiz de dados do SVM devem estar em um agregado espelhado. Não é possível mover esses volumes para um agregado sem espelhamento. Se eles estiverem em um agregado sem espelhamento, as operações de comutação negociadas e switchback serão vetadas. O comando MetroCluster check fornece um aviso se for esse o caso.

Considerações para agregados sem espelhamento e SVMs

Os SVMs devem ser configurados somente em agregados espelhados ou somente em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados pode resultar em uma operação de switchover que excede 120 segundos e resultar em uma interrupção de dados se os agregados sem espelhamento não ficarem online.

Considerações para agregados sem espelhamento e SAN

Nas versões ONTAP anteriores a 9,9.1, um LUN não deve ser localizado em um agregado sem espelhamento. Configurar um LUN em um agregado sem espelhamento pode resultar em uma operação de switchover que excede 120 segundos e uma interrupção de dados.

Uso de firewall em sites da MetroCluster

Considerações sobre o uso de firewall em sites da MetroCluster

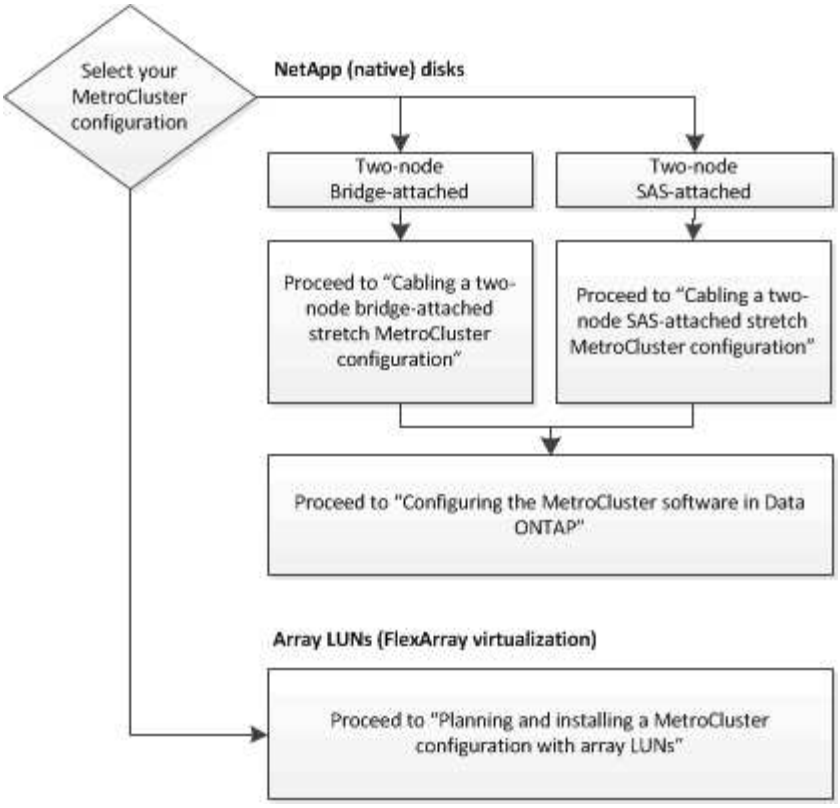
Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o acesso às portas necessárias.

A tabela a seguir mostra o uso da porta TCP/UDP em um firewall externo posicionado entre dois sites do MetroCluster.

Tipo de trânsito	Porta/serviços
Peering de clusters	11104 / TCP 11105 / TCP
Gerente do sistema da ONTAP	443 / TCP
LIFs IP entre clusters do MetroCluster	65200 / TCP 10006 / TCP e UDP
Assistência ao hardware	4444 / TCP

Escolhendo o procedimento de instalação correto para sua configuração

Você deve escolher o procedimento de instalação correto com base no uso de LUNs FlexArray e na forma como os controladores de storage se conetam às gavetas de storage.

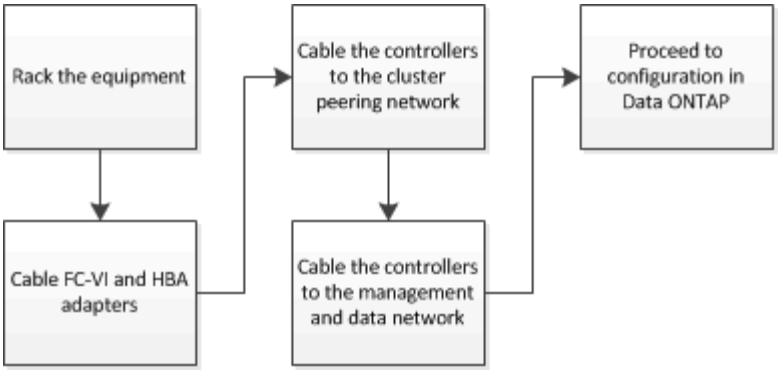


Para este tipo de instalação…	Utilize estes procedimentos…
Configuração elástica de dois nós com pontes FC para SAS	1. "Cabeamento de uma configuração Stretch MetroCluster de dois nós conetada em ponte" 2. "Configurando o software MetroCluster no ONTAP"
Configuração elástica de dois nós com cabeamento SAS de conexão direta	1. "Cabeamento de uma configuração Stretch MetroCluster com conexão SAS de dois nós" 2. "Configurando o software MetroCluster no ONTAP"
Instalação com LUNs de array	"Conexões em configurações Stretch MetroCluster com LUNs de array"

Cabo uma configuração Stretch MetroCluster de dois nós conetada a SAS

Cabeamento de uma configuração Stretch MetroCluster com conexão SAS de dois nós

Os componentes do MetroCluster devem ser fisicamente instalados, cabeados e configurados em ambos os locais geográficos. As etapas são ligeiramente diferentes para um sistema com compartimentos de disco nativos, em vez de um sistema com LUNs de array.



Partes de uma configuração Stretch MetroCluster de dois nós conetada a SAS

A configuração de conexão SAS com MetroCluster de dois nós requer várias peças, incluindo dois clusters de nó único nos quais os controladores de storage são diretamente conectados ao storage usando cabos SAS.

A configuração do MetroCluster inclui os seguintes elementos-chave de hardware:

- Controladores de storage

  Os controladores de storage se conetam diretamente ao storage usando cabos SAS.

  Cada controlador de storage é configurado como parceiro de recuperação de desastres para um controlador de storage no local do parceiro.

  - Cabos SAS de cobre podem ser usados para distâncias mais curtas.
  - Os cabos SAS óticos podem ser usados para distâncias mais longas.

  > Em sistemas que usam LUNs de array e-Series, os controladores de storage podem ser diretamente conectados aos storage arrays e-Series. Para outros LUNs de array, são necessárias conexões por meio de switches FC.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Rede de peering de cluster

  A rede de peering de cluster fornece conetividade para espelhamento da configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.

Componentes de hardware MetroCluster necessários e diretrizes de nomenclatura para configurações de stretch com conexão SAS de dois nós

A configuração do MetroCluster requer uma variedade de componentes de hardware. Para conveniência e clareza, os nomes padrão dos componentes são usados em toda a

documentação do MetroCluster. Um site é referido como Site A e o outro site é referido como Site B.

Software e hardware suportados

O hardware e o software devem ser compatíveis com a configuração MetroCluster FC.

"NetApp Hardware Universe"

Ao usar sistemas AFF, todos os módulos do controlador na configuração do MetroCluster devem ser configurados como sistemas AFF.

Redundância de hardware na configuração MetroCluster

Devido à redundância de hardware na configuração do MetroCluster, há dois de cada componente em cada local. Os sites são arbitrariamente atribuídos às letras A e B e os componentes individuais são arbitrariamente atribuídos aos números 1 e 2.

Dois clusters ONTAP de nó único

A configuração Stretch MetroCluster conectada ao SAS requer dois clusters ONTAP de nó único.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Dois módulos de controlador de armazenamento

A configuração Stretch MetroCluster conetada a SAS requer dois módulos de controlador de armazenamento.

- A nomeação deve ser única dentro da configuração do MetroCluster.
- Todos os módulos do controlador na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.
- Todos os módulos de controladora em um grupo de DR devem ter o mesmo modelo.
- Todos os módulos de controladora em um grupo de DR devem usar a mesma configuração FC-VI.

  Alguns módulos de controladora suportam duas opções de conectividade FC-VI:

  - Portas FC-VI integradas
  - Uma placa FC-VI no slot 1

    Uma combinação de um módulo de controladora que usa portas FC-VI integradas e outra que usa uma placa FC-VI complementar não é compatível. Por exemplo, se um nó usar a configuração FC-VI integrada, todos os outros nós do grupo de DR também precisarão usar a configuração FC-VI integrada.

Nomes de exemplo:

- Local A: Controller_A_1

- Local B: Controller_B_1

Pelo menos quatro compartimentos de disco SAS (recomendado)

A configuração Stretch MetroCluster conectada a SAS requer pelo menos duas gavetas de disco SAS. Recomenda-se quatro compartimentos de disco SAS.

Duas gavetas são recomendadas em cada local para permitir a propriedade de disco por compartimento. Há suporte para um mínimo de uma prateleira em cada local.

Nomes de exemplo:

- Local A:
  - shelf_A_1_1
  - shelf_A_1_2
- Local B:
  - shelf_B_1_1
  - shelf_B_1_2

Misturando módulos IOM12 e IOM 6 em uma pilha

Sua versão do ONTAP deve suportar a mistura de prateleiras. Consulte a ferramenta de Matriz de interoperabilidade (IMT) para ver se a sua versão do ONTAP suporta a mistura de prateleiras. "IMT"

Para obter mais detalhes sobre a mistura de prateleiras, consulte: "Gavetas de adição dinâmica com IOM12 módulos para uma stack de gavetas com IOM6 módulos"

Instale e faça o cabo dos componentes MetroCluster para configurações de alongamento de dois nós conetadas a SAS

Instalação e cabeamento de componentes MetroCluster para configurações de alongamento de dois nós conetadas a SAS

Os controladores de storage devem ser cabeados para a Mídia de storage e entre si. Os controladores de storage também devem ser cabeados para a rede de dados e gerenciamento.

Antes de iniciar qualquer procedimento neste documento

Os seguintes requisitos gerais devem ser atendidos antes de concluir esta tarefa:

- Antes da instalação, você deve se familiarizar com as considerações e as práticas recomendadas para instalação e cabeamento de compartimentos de disco para o modelo de compartimento de disco.
- Todos os componentes do MetroCluster devem ser suportados.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

Sobre esta tarefa

- Os termos nó e controlador são usados de forma intercambiável.

Colocar em pilha os componentes de hardware

Se você não recebeu o equipamento já instalado em armários, você deve colocar os componentes em rack.

Esta tarefa tem de ser executada em ambos os sites da MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   A quantidade de espaço em rack necessária depende do modelo de plataforma das controladoras de storage, dos tipos de switch e do número de stacks de compartimento de disco na configuração.

2. Utilizando práticas de oficina padrão para trabalhar com equipamentos elétricos, certifique-se de que está devidamente ligado à terra.
3. Instale os controladores de armazenamento no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Instale as gavetas de disco, encadeie em série as gavetas de disco em cada pilha, ligue-as e defina as IDs de gaveta.

   Consulte o guia apropriado para o modelo do compartimento de disco para obter informações sobre prateleiras de disco em encadeamento em série e sobre a configuração de IDs de gaveta.

   As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais). Ao definir manualmente as IDs de gaveta, você deve desligar o compartimento de disco.

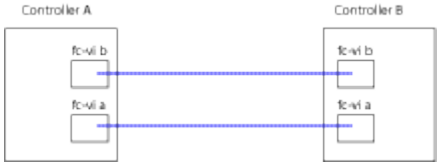
Fazer o cabeamento das controladoras umas para as outras e das gavetas de storage

Os adaptadores FC-VI da controladora devem ser cabeados diretamente entre si. As portas SAS da controladora devem ser cabeadas para as stacks de storage remoto e local.

Esta tarefa deve ser executada em ambos os locais do MetroCluster.

Passos

1. Cable as portas FC-VI.

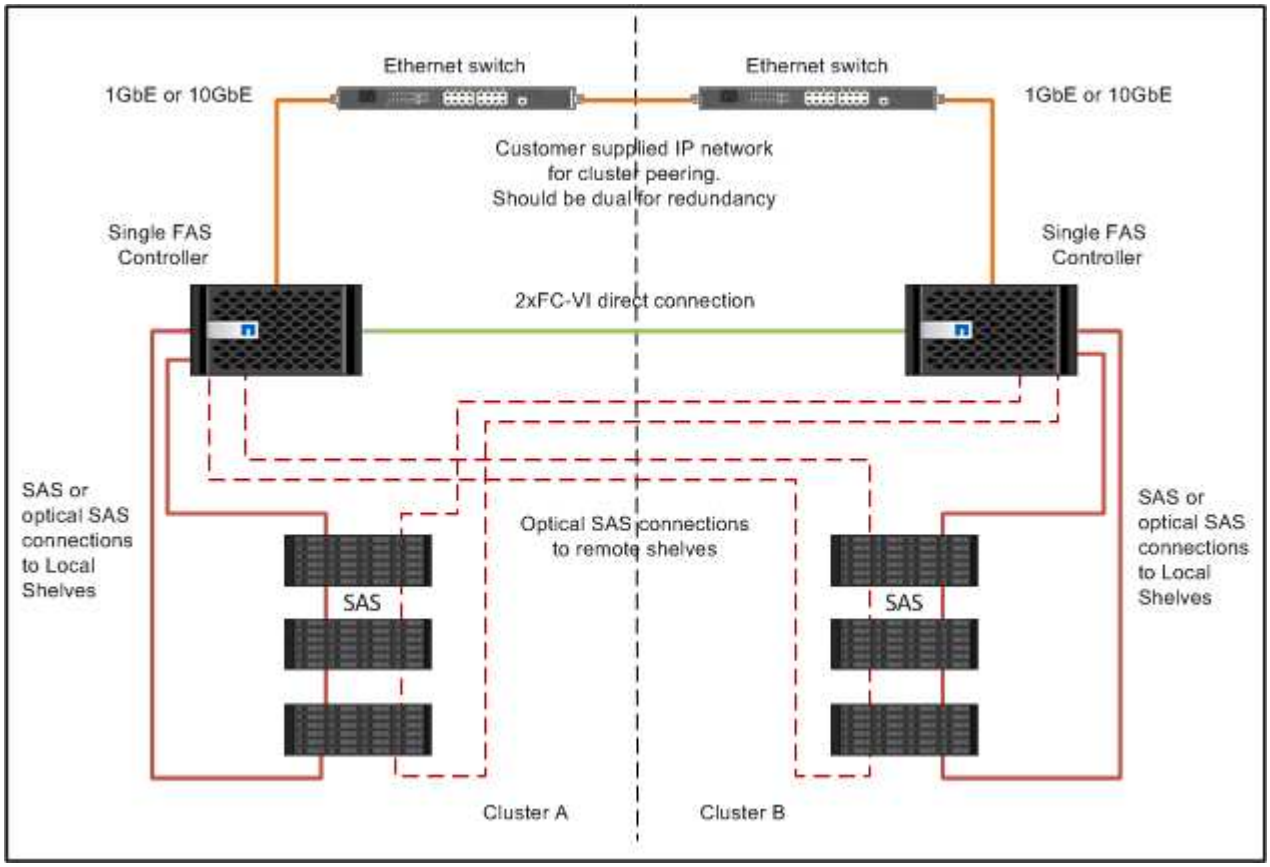


   A ilustração acima é uma conexão de cabo representativa típica. As portas FC-VI específicas variam de acordo com o módulo do controlador.

- Os módulos de controladora FAS8200 e AFF A300 podem ser solicitados com uma das duas opções de conectividade FC-VI:
  - As portas integradas 0e e 0f são configuradas no modo FC-VI.
  - As portas 1a e 1b em uma placa FC-VI entram no slot 1.
- Os módulos dos controladores de sistemas de storage AFF A700 e FAS9000 usam quatro portas FC-VI cada uma.
- Os módulos de controladora do sistema de storage AFF A400 e FAS8300 usam as portas FC-VI 2a e 2b.

2. Faça o cabo das portas SAS.

A ilustração a seguir mostra as conexões. O uso da porta pode ser diferente dependendo das portas SAS e FC-VI disponíveis no módulo da controladora.



Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de cluster para que eles tenham conetividade com o cluster no local do parceiro.

Esta tarefa deve ser executada em cada módulo do controlador na configuração do MetroCluster.

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

Passos

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

   O peering de cluster pode ser feito em portas dedicadas ou em portas de dados. O uso de portas dedicadas fornece uma taxa de transferência mais alta para o tráfego de peering de cluster.

   "Configuração expressa de peering de cluster e SVM"

Cabeamento das conexões de dados e gerenciamento

Você deve encaminhar as portas de gerenciamento e dados em cada controlador de storage para as redes do local.

Esta tarefa deve ser repetida para cada novo controlador em ambos os locais do MetroCluster.

Pode ligar as portas de gestão do controlador e do comutador de cluster a comutadores existentes na rede. Além disso, você pode conetar o controlador a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passos

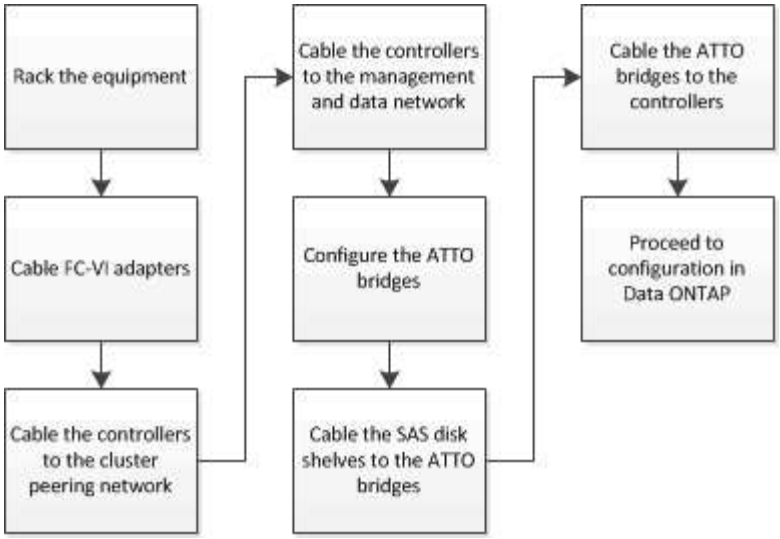
1. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

   "Documentação dos sistemas de hardware da ONTAP"

Cable uma configuração Stretch MetroCluster com conexão em ponte de dois nós

Cabeamento de uma configuração Stretch MetroCluster de dois nós conetada em ponte

Os componentes do MetroCluster devem ser fisicamente instalados, cabeados e configurados em ambos os locais geográficos. As etapas são ligeiramente diferentes para um sistema com compartimentos de disco nativos, em vez de um sistema com LUNs de array.



Partes de uma configuração Stretch MetroCluster de dois nós conetada em ponte

Ao Planejar sua configuração do MetroCluster, você deve entender as partes da configuração e como elas funcionam juntas.

A configuração do MetroCluster inclui os seguintes elementos-chave de hardware:

- Controladores de storage

  As controladoras de storage não são conectadas diretamente ao storage, mas conectadas a pontes FC para SAS. Os controladores de storage são conectados por cabos FC entre os adaptadores FC-VI de cada controlador.

  Cada controlador de storage é configurado como parceiro de recuperação de desastres para um controlador de storage no local do parceiro.

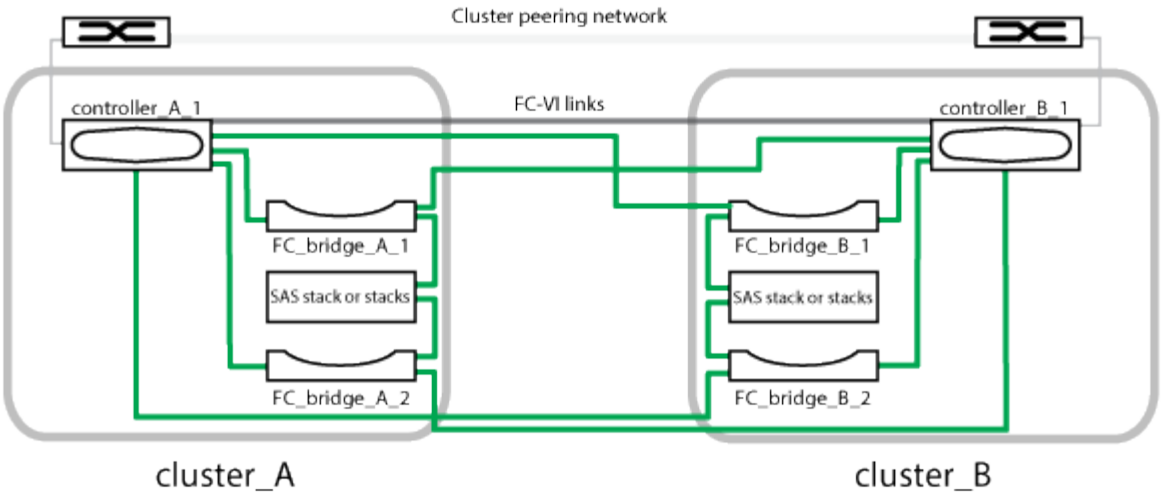
- Pontes FC para SAS

  As pontes FC para SAS conectam as stacks de storage SAS às portas iniciadores de FC nas controladoras, fornecendo uma ponte entre os dois protocolos.

- Rede de peering de cluster

  A rede de peering de cluster fornece conetividade para espelhamento da configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.

A ilustração a seguir mostra uma visualização simplificada da configuração do MetroCluster. Para algumas conexões, uma única linha representa várias conexões redundantes entre os componentes. As conexões de rede de gerenciamento e dados não são mostradas.



- A configuração consiste em dois clusters de nó único.
- Cada local tem uma ou mais pilhas de storage SAS.

> Gavetas SAS em configurações MetroCluster não são compatíveis com cabeamento ACP.

São suportadas stacks de armazenamento adicionais, mas apenas uma é mostrada em cada local.

Componentes de hardware necessários da MetroCluster e convenções de nomenclatura para configurações de stretch anexadas a ponte de dois nós

Ao Planejar sua configuração do MetroCluster, você deve entender os componentes de hardware e software necessários e suportados. Para conveniência e clareza, você também deve entender as convenções de nomenclatura usadas para componentes em exemplos ao longo da documentação. Por exemplo, um site é referido como Site A e o outro site é referido como Site B.

Software e hardware suportados

O hardware e o software devem ser compatíveis com a configuração MetroCluster FC.

"NetApp Hardware Universe"

Ao usar sistemas AFF, todos os módulos do controlador na configuração do MetroCluster devem ser configurados como sistemas AFF.

Redundância de hardware na configuração MetroCluster

Devido à redundância de hardware na configuração do MetroCluster, há dois de cada componente em cada local. Os sites são arbitrariamente atribuídos às letras A e B e os componentes individuais são arbitrariamente atribuídos aos números 1 e 2.

Requisito para dois clusters ONTAP de nó único

A configuração Stretch MetroCluster conectada a ponte requer dois clusters ONTAP de nó único.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Requisito para dois módulos de controlador de armazenamento

A configuração Stretch MetroCluster conetada em ponte requer dois módulos de controlador de armazenamento.

Os controladores devem atender aos seguintes requisitos:

- A nomeação deve ser única dentro da configuração do MetroCluster.
- Todos os módulos do controlador na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.
- Todos os módulos de controladora em um grupo de DR devem ter o mesmo modelo.
- Todos os módulos de controladora em um grupo de DR devem usar a mesma configuração FC-VI.

  Alguns módulos de controladora suportam duas opções de conectividade FC-VI:

  - Portas FC-VI integradas
  - Uma placa FC-VI no slot 1

    Uma combinação de um módulo de controladora que usa portas FC-VI integradas e outra que usa uma placa FC-VI complementar não é compatível. Por exemplo, se um nó usar a configuração FC-VI integrada, todos os outros nós do grupo de DR também precisarão usar a configuração FC-VI integrada.

Nomes de exemplo:

- Local A: Controller_A_1
- Local B: Controller_B_1

Requisito para pontes FC para SAS

A configuração Stretch MetroCluster conectada em ponte requer duas ou mais pontes FC para SAS em cada local.

Essas pontes conetam os compartimentos de disco SAS aos módulos da controladora.

> As bridges FibreBridge 6500N não são suportadas em configurações que executam o ONTAP 9.8 e posterior.

- As pontes FibreBridge 7600N e 7500N suportam até quatro stacks SAS.
- Cada stack pode usar modelos diferentes de IOM, mas todas as gavetas de uma stack precisam usar o mesmo modelo.

  Os modelos IOM suportados dependem da versão ONTAP que você está executando.

- A nomeação deve ser única dentro da configuração do MetroCluster.

Os nomes sugeridos usados como exemplos neste procedimento identificam o módulo do controlador ao qual a ponte se coneta e a porta.

Nomes de exemplo:

- Local A:
  - ponte_A_1_*port-number*
  - ponte_A_2_*port-number*
- Local B:
  - ponte_B_1_*port-number*
  - ponte_B_2_*port-number*

Requisito para pelo menos quatro gavetas SAS (recomendado)

A configuração Stretch MetroCluster conetada em ponte requer pelo menos duas gavetas SAS. No entanto, duas gavetas são recomendadas em cada local para permitir a propriedade de disco por compartimento, totalizando quatro gavetas SAS.

Há suporte para um mínimo de uma prateleira em cada local.

Nomes de exemplo:

- Local A:
  - shelf_A_1_1
  - shelf_A_1_2
- Local B:
  - shelf_B_1_1
  - shelf_B_1_2

Misturando módulos IOM12 e IOM 6 em uma pilha

Sua versão do ONTAP deve suportar a mistura de prateleiras. Consulte a ferramenta de Matriz de interoperabilidade (IMT) para ver se a sua versão do ONTAP suporta a mistura de prateleiras. "IMT"

Para obter mais detalhes sobre a mistura de prateleiras, consulte: "Gavetas de adição dinâmica com IOM12 módulos para uma stack de gavetas com IOM6 módulos"

Planilha de coleta de informações para bridges FC-para-SAS

Antes de começar a configurar os sites do MetroCluster, você deve coletar as informações de configuração necessárias.

Local A, ponte FC-para-SAS 1 (FC_bridge_A_1a)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte se coneta ao Controller_A_1_*port-number* e Controller_B_1_*port-number*.

Local A	O seu valor
Endereço IP Bridge_A_1a	
Nome de utilizador Bridge_A_1a	
Senha Bridge_A_1a	

Local A, ponte FC-para-SAS 2 (FC_bridge_A_1b)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte se coneta ao Controller_A_1_*port-number* e Controller_B_1_*port-number*.

Local A	O seu valor
Endereço IP Bridge_A_1b	
Nome de utilizador Bridge_A_1b	
Senha Bridge_A_1b	

Local B, ponte FC-para-SAS 1 (FC_bridge_B_1a)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte coneta-se ao Controller_A_1_*port-number' e Controller_B_1____port-number*.

Local B	O seu valor
Endereço IP Bridge_B_1a	
Nome de utilizador Bridge_B_1a	
Bridge_B_1a Palavra-passe	

Local B, ponte FC-para-SAS 2 (FC_bridge_B_1b)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte coneta-se ao Controller_A_1_*port-number' e Controller_B_1____port-number*.

Local B	O seu valor
Endereço IP Bridge_B_1b	
Nome de utilizador Bridge_B_1b	

Bridge_B_1b Palavra-passe	

Instale e faça o cabo dos componentes do MetroCluster

Colocar em pilha os componentes de hardware

Se você não recebeu o equipamento já instalado em armários, você deve colocar os componentes em rack.

Esta tarefa tem de ser executada em ambos os sites da MetroCluster.

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

   O espaço em rack depende do modelo de plataforma dos controladores de storage, dos tipos de switch e do número de stacks de compartimento de disco na sua configuração.

2. Aterre-se corretamente.
3. Instale os controladores de armazenamento no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Instale as gavetas de disco, ligue-as e defina as IDs de gaveta.
   - É necessário desligar cada compartimento de disco.
   - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
5. Instalar cada ponte FC para SAS:

   a. Fixe os suportes "L" na parte frontal da ponte à frente do rack (montagem embutida) com os quatro parafusos.

      As aberturas nos suportes da ponte "L" estão em conformidade com o padrão de rack ETA-310-X para racks de 19 polegadas (482,6 mm).

      Para obter mais informações e uma ilustração da instalação, consulte o *ATTO FibreBridge Installation and Operation Manual para o seu modelo de ponte*.

   b. Conete cada ponte a uma fonte de alimentação que forneça um aterramento adequado.
   c. Ligue cada ponte.

      Para obter a resiliência máxima, as bridges que estão conectadas à mesma stack de shelves de disco devem ser conectadas a diferentes fontes de energia.

   O LED bridge Ready pode demorar até 30 segundos a acender, indicando que a ponte concluiu a sequência de autoteste de ativação.

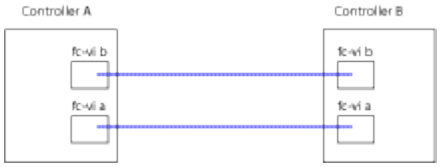
Fazer o cabeamento das controladoras umas para as outras

Os adaptadores FC-VI de cada controladora devem ser cabeados diretamente ao

parceiro.

Passos

1. Cable as portas FC-VI.



A ilustração acima é uma representação típica do cabeamento necessário. As portas FC-VI específicas variam de acordo com o módulo do controlador.

- Os módulos de controladora AFF A300 e FAS8200 podem ser solicitados com uma das duas opções de conectividade FC-VI:
  - Portas integradas 0e e 0f configuradas no modo FC-VI.
  - Portas 1a e 1b em uma placa FC-VI no slot 1.
- Os módulos dos controladores de sistemas de storage AFF A700 e FAS9000 usam quatro portas FC-VI cada uma.

Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de cluster para que eles tenham conetividade com o cluster no local do parceiro.

Esta tarefa deve ser executada em cada módulo do controlador na configuração do MetroCluster.

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

Passos

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

   O peering de cluster pode ser feito em portas dedicadas ou em portas de dados. O uso de portas dedicadas fornece uma taxa de transferência mais alta para o tráfego de peering de cluster.

   "Configuração expressa de peering de cluster e SVM"

Cabeamento das conexões de dados e gerenciamento

Você deve encaminhar as portas de gerenciamento e dados em cada controlador de storage para as redes do local.

Esta tarefa deve ser repetida para cada novo controlador em ambos os locais do MetroCluster.

Pode ligar as portas de gestão do controlador e do comutador de cluster a comutadores existentes na rede. Além disso, você pode conetar o controlador a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passos

1. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

   "Documentação dos sistemas de hardware da ONTAP"

Instalar pontes FC a SAS e gavetas de disco SAS

Instale e faça o cabeamento das pontes ATTO FibreBridge e das gavetas de disco SAS quando você adicionar novo armazenamento à configuração.

Sobre esta tarefa

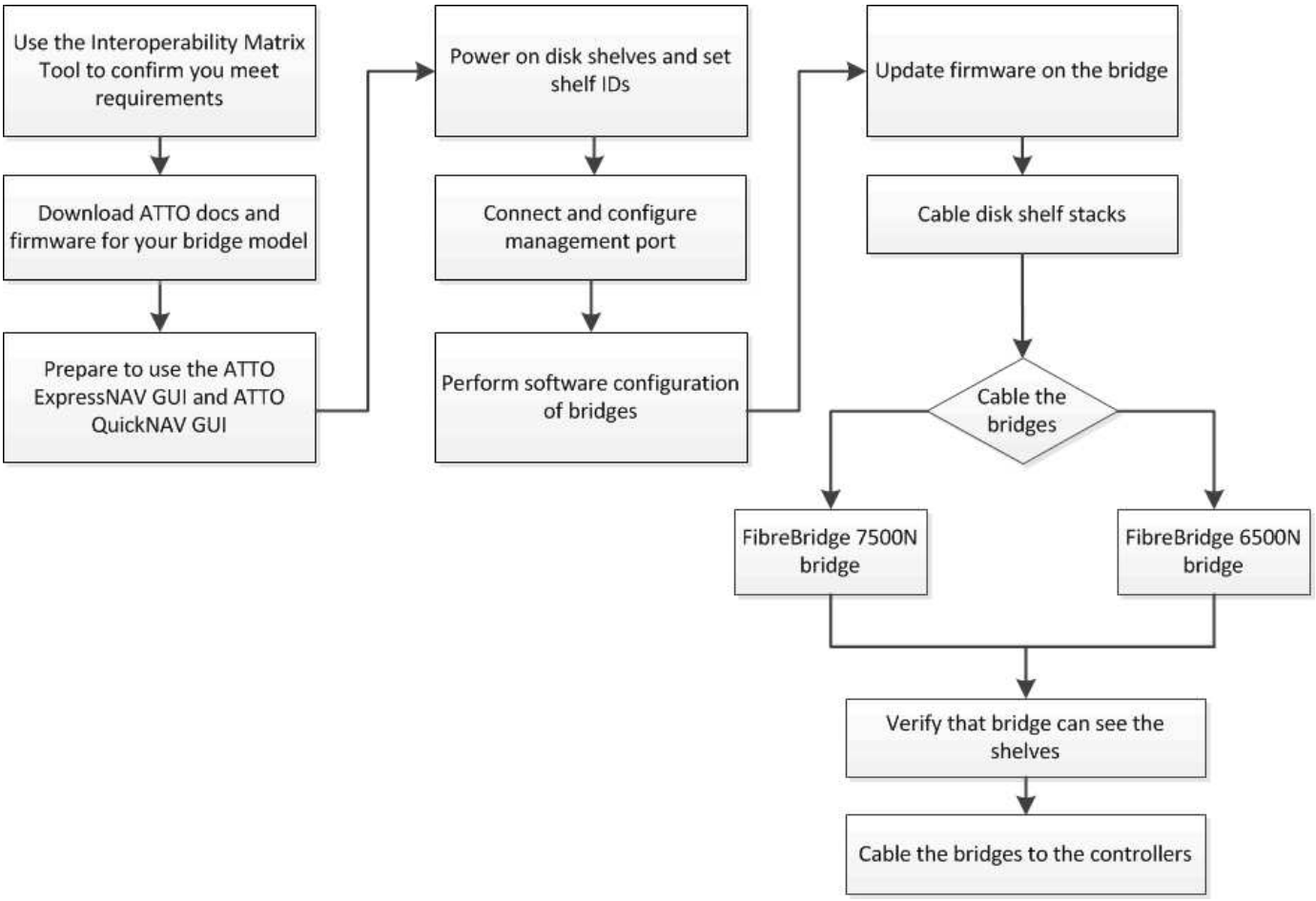
Para sistemas recebidos de fábrica, as pontes FC para SAS são pré-configuradas e não exigem configuração adicional.

Este procedimento é escrito com a suposição de que você está usando as interfaces de gerenciamento de bridge recomendadas: A GUI ATTO ExpressNAV e o utilitário ATTO Quicknav.

Você usa a GUI ATTO ExpressNAV para configurar e gerenciar uma bridge e atualizar o firmware da bridge. Você usa o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet bridge.

Em vez disso, você pode usar outras interfaces de gerenciamento, se necessário, como uma porta serial ou Telnet para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet e FTP para atualizar o firmware da ponte.

Este procedimento utiliza o seguinte fluxo de trabalho:



Gerenciamento na banda das pontes FC para SAS

Começando com o ONTAP 9.5 com o FibreBridge 7500N ou 7600N bridges, *in-band Management* das bridges é suportado como uma alternativa ao gerenciamento IP das bridges. A partir do ONTAP 9.8, o gerenciamento fora da banda está obsoleto.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Ao usar o gerenciamento na banda, as bridges podem ser gerenciadas e monitoradas a partir da CLI do ONTAP usando a conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário, reduzindo a vulnerabilidade de segurança da ponte.

A disponibilidade do gerenciamento em banda das pontes depende da versão do ONTAP:

- A partir do ONTAP 9.8, as bridges são gerenciadas por meio de conexões na banda por padrão e o gerenciamento fora da banda das bridges via SNMP é obsoleto.
- ONTAP 9.5 a 9,7: O gerenciamento na banda ou o gerenciamento SNMP fora da banda é suportado.
- Antes do ONTAP 9,5, somente o gerenciamento SNMP fora da banda é suportado.

Os comandos Bridge CLI podem ser emitidos a partir do comando ONTAP interface `storage bridge run-cli -name <bridge_name> -command <bridge_command_name>` na interface ONTAP.

O uso do gerenciamento na banda com acesso IP desativado é recomendado para melhorar a segurança limitando a conetividade física da ponte.

Limites e regras de anexo da ponte FibreBridge 7600N e 7500N

Reveja os limites e considerações ao anexar pontes FibreBridge 7600N e 7500N.

Limites das pontes FibreBridge 7600N e 7500N

- O número máximo de unidades HDD e SSD combinadas é 240.
- O número máximo de unidades SSD é 96.
- O número máximo de SSDs por porta SAS é 48.
- O número máximo de gavetas por porta SAS é de 10.

Regras de anexo de ponte FibreBridge 7600N e 7500N

- Não misture unidades SSD e HDD na mesma porta SAS.
- Distribua as gavetas uniformemente entre as portas SAS.
- Você não deve ter DS460 gavetas na mesma porta SAS que outros tipos de gaveta (por exemplo, DS212 ou DS224 gavetas).

Exemplo de configuração

A seguir mostra um exemplo de configuração para conectar quatro gavetas DS224 com unidades SSD e seis gavetas DS224 com unidades HDD:

Porta de SAS	Compartimentos e unidades
Porta SAS A	2x DS224 gavetas com unidades SSD
Porta SAS-B	2x DS224 gavetas com unidades SSD
Porta SAS-C	3x DS224 gavetas com unidades HDD
Porta SAS-D	3x DS224 gavetas com unidades HDD

Prepare-se para a instalação

Quando estiver se preparando para instalar as bridges como parte do seu novo sistema MetroCluster, verifique se o sistema atende a certos requisitos, incluindo atender aos requisitos de configuração e configuração das bridges. Outros requisitos incluem o download dos documentos necessários, o utilitário ATTO Quicknav e o firmware da ponte.

Antes de começar

- Seu sistema já deve ser instalado em um rack se ele não foi enviado em um gabinete do sistema.
- Sua configuração deve estar usando modelos de hardware e versões de software compatíveis.

  No "Ferramenta de Matriz de interoperabilidade NetApp (IMT)", você pode usar o campo **solução de armazenamento** para selecionar sua solução MetroCluster. Você pode usar o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode selecionar **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Cada controlador FC precisa ter uma porta FC disponível para uma ponte para se conectar a ele.

- Você deve estar familiarizado com como lidar com cabos SAS e com os considerações e práticas recomendadas para a instalação e o cabeamento das gavetas de disco.

  O *Installation and Service Guide* do modelo de compartimento de disco descreve as considerações e as práticas recomendadas.

- O computador que você está usando para configurar as bridges deve estar executando um navegador da Web compatível com ATTO para usar a GUI ATTO ExpressNAV.

  As Notas de versão do produto *ATTO* têm uma lista atualizada de navegadores da Web compatíveis. Você pode acessar este documento a partir do SITE DA ATTO, conforme descrito nas etapas a seguir.

Passos

1. Faça o download do *Installation and Service Guide* do modelo do compartimento de disco:
   a. Acesse o site DA ATTO usando o link fornecido para o modelo do FibreBridge e baixe o manual e o utilitário Quicknav.

      O *ATTO FibreBridge Installation and Operation Manual* para sua ponte de modelo tem mais informações sobre interfaces de gerenciamento.

      Você pode acessar este e outros conteúdos no SITE DA ATTO usando o link fornecido na página Descrição DO ATTO Fibrebridge.

2. Reúna o hardware e as informações necessárias para usar as interfaces de gerenciamento de bridge recomendadas, a GUI ATTO ExpressNAV e o utilitário ATTO Quicknav:
   a. Determine um nome de usuário e uma senha não padrão (para acessar as pontes).

      Você deve alterar o nome de usuário e a senha padrão.

   b. Se estiver configurando para gerenciamento IP das pontes, você precisará do cabo Ethernet blindado fornecido com as pontes (que se coneta da porta 1 de gerenciamento Ethernet da ponte à sua rede).
   c. Se estiver configurando para gerenciamento IP das bridges, você precisará de um endereço IP, máscara de sub-rede e informações de gateway para a porta 1 de gerenciamento Ethernet em cada bridge.
   d. Desative os clientes VPN no computador que você está usando para configuração.

      Os clientes VPN ativos fazem com que o Quicknav procure por bridges falhem.

Instalar a ponte FC para SAS e as gavetas SAS

Depois de garantir que o sistema atenda a todos os requisitos em "preparando-se para a instalação", você pode instalar seu novo sistema.

Sobre esta tarefa

- A configuração do disco e do compartimento em ambos os locais deve ser idêntica.

  Se um agregado não espelhado for usado, a configuração de disco e compartimento em cada local pode ser diferente.

Todos os discos do grupo de recuperação de desastres devem usar o mesmo tipo de conexão e estar visíveis para todos os nós do grupo de recuperação de desastres, independentemente dos discos usados para agregado espelhado ou não espelhado.

- Os requisitos de conetividade do sistema para distâncias máximas para compartimentos de disco, controladores FC e dispositivos de fita de backup usando cabos de fibra ótica multimodo de 50 mícrones, também se aplicam a pontes FibreBridge.

  "NetApp Hardware Universe"

- Uma combinação de IOM12 módulos e IOM3 módulos não é suportada na mesma pilha de storage. Uma combinação de IOM12 módulos e IOM6 módulos é compatível com a mesma pilha de storage se o sistema estiver executando uma versão compatível do ONTAP.

O ACP na banda é compatível sem cabeamento adicional nas seguintes gavetas e ponte FibreBridge 7500N ou 7600N:

- IOM12 (DS460C) atrás de uma ponte de 7500N ou 7600N com ONTAP 9.2 e posterior
- IOM12 (DS212C e DS224C) atrás de uma ponte 7500N ou 7600N com ONTAP 9.1 e posterior

As gavetas SAS em configurações de MetroCluster não são compatíveis com cabeamento ACP.

Ative o acesso à porta IP na ponte FibreBridge 7600N, se necessário

Se você estiver usando uma versão do ONTAP anterior a 9,5, ou de outra forma planeja usar o acesso fora da banda à ponte FibreBridge 7600N usando telnet ou outros protocolos e serviços de porta IP (FTP, ExpressNAV, ICMP ou Quicknav), você pode ativar os serviços de acesso através da porta do console.

Sobre esta tarefa

Ao contrário das pontes ATTO FibreBridge 7500N, a ponte FibreBridge 7600N é fornecida com todos os protocolos e serviços de porta IP desativados.

A partir do ONTAP 9.5, *gerenciamento na banda* das bridges é suportado. Isso significa que as pontes podem ser configuradas e monitoradas a partir da CLI do ONTAP por meio da conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário e as interfaces do usuário da ponte não são necessárias.

A partir do ONTAP 9.8, *gerenciamento na banda* das bridges é suportado por padrão e o gerenciamento SNMP fora da banda é obsoleto.

Essa tarefa é necessária se você estiver usando **não** o gerenciamento na banda para gerenciar as bridges. Neste caso, você precisa configurar a ponte através da porta de gerenciamento Ethernet.

Passos

1. Acesse a interface do console de ponte conetando um cabo serial à porta serial na ponte FibreBridge 7600N.
2. Usando o console, ative os serviços de acesso e salve a configuração:

```
set closeport none
```

```
saveconfiguration
```

O `set closeport none` comando habilita todos os serviços de acesso na ponte.

3. Desative um serviço, se desejado, emitindo o `set closeport` comando e repetindo o comando conforme necessário até que todos os serviços desejados sejam desativados:

   ```
   set closeport service
   ```

   O `set closeport` comando desativa um único serviço de cada vez.

   O parâmetro *`service`* pode ser especificado como um dos seguintes:

   - expressarsnav
   - ftp
   - icmp
   - navegação rápida
   - snmp
   - telnet

   Pode verificar se um protocolo específico está ativado ou desativado utilizando o `get closeport` comando.

4. Se você estiver habilitando o SNMP, você também deve emitir o seguinte comando:

   ```
   set SNMP enabled
   ```

   SNMP é o único protocolo que requer um comando de ativação separado.

5. Guardar a configuração:

   ```
   saveconfiguration
   ```

Configurar as pontes FC para SAS

Antes de fazer o cabeamento do modelo das pontes FC para SAS, você deve configurar as configurações no software FibreBridge.

Antes de começar

Você deve decidir se vai usar o gerenciamento em banda das pontes.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Sobre esta tarefa

Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

Passos

1. Configure a porta do console serial no ATTO FibreBridge definindo a velocidade da porta para 115000 bauds:

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

   A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.

3. Se estiver configurando para gerenciamento IP, conete a porta 1 de gerenciamento Ethernet em cada bridge à rede usando um cabo Ethernet.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   A porta 1 de gerenciamento Ethernet permite que você baixe rapidamente o firmware da ponte (usando interfaces de gerenciamento ATTO ExpressNAV ou FTP) e recupere arquivos principais e extraia logs.

4. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual* para o modelo de bridge.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

5. Configure a ponte.

   Você deve anotar o nome de usuário e a senha que você designar.

Não configure a sincronização de tempo no ATTO FibreBridge 7600N ou 7500N. A sincronização de tempo para O ATTO FibreBridge 7600N ou 7500N é definida para a hora do cluster depois que a ponte é descoberta pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

   Se estiver usando a CLI, você deve executar os seguintes comandos:

   ```
   set ipaddress mp1 ip-address

   set ipsubnetmask mp1 subnet-mask

   set ipgateway mp1 x.x.x.x

   set ipdhcp mp1 disabled

   set ethernetspeed mp1 1000
   ```

b. Configure o nome da ponte.

   As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

   Exemplos de nomes de bridge para um grupo de pilha em cada local:

   - bridge_A_1a
   - bridge_A_1b
   - bridge_B_1a
   - bridge_B_1b

   Se estiver usando a CLI, você deve executar o seguinte comando:

   ```
   set bridgename <bridge_name>
   ```

c. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte:

   ```
   set SNMP enabled
   ```

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

6. Configurar as portas FC de ponte.

   a. Configure a taxa/velocidade de dados das portas FC em ponte.

A taxa de dados FC suportada depende da ponte do modelo.

- A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
- A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.

> A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pela porta FC do módulo do controlador à qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCDataRate <port-number> <port-speed>
```

b. Se você estiver configurando uma ponte FibreBridge 7500N, configure o modo de conexão que a porta usa para "ptp".

> A configuração FCConnMode não é necessária ao configurar uma ponte FibreBridge 7600N.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCConnMode <port-number> ptp
```

c. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, você deve configurar ou desativar a porta FC2.

- Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.
- Se você não estiver usando a segunda porta, então você deve desativar a porta:

  ```
  FCPortDisable <port-number>
  ```

O exemplo a seguir mostra a desativação da porta FC 2:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, desative as portas SAS não utilizadas:

```
SASPortDisable sas-port
```

> As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas.

Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas. O exemplo a seguir mostra a desativação da porta SAS B. você deve desabilitar as portas SAS C e D da mesma forma:

```
SASPortDisable b

SAS Port B has been disabled.
```

7. Proteja o acesso à ponte e salve a configuração da ponte. Escolha uma opção abaixo, dependendo da versão do ONTAP que seu sistema está sendo executado.

Versão de ONTAP	Passos
ONTAP 9 1.5 ou posterior	a. Veja o status das pontes: `storage bridge show` A saída mostra qual ponte não está protegida. b. Fixe a ponte: `securebridge`
ONTAP 9 1.4 ou anterior	a. Veja o status das pontes: `storage bridge show` A saída mostra qual ponte não está protegida. b. Verifique o estado das portas da ponte não protegida: `info` A saída mostra o status das portas Ethernet MP1 e MP2. c. Se a porta Ethernet MP1 estiver ativada, execute: `set EthernetPort mp1 disabled` Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2. d. Salve a configuração da ponte. Você deve executar os seguintes comandos: `SaveConfiguration` `FirmwareRestart` Você é solicitado a reiniciar a ponte.

8. Depois de concluir a configuração do MetroCluster, use o `flashimages` comando para verificar sua versão do firmware do FibreBridge e, se as bridges não estiverem usando a versão mais recente

suportada, atualize o firmware em todas as bridges na configuração.

"Mantenha os componentes do MetroCluster"

Cable disk shelves to the bridges

Você precisa usar as pontes FC para SAS corretas para fazer o cabeamento das gavetas de disco.

Opções

- Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando IOM12 módulos
- Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando módulos IOM6 ou IOM3

Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras de disco usando IOM12 módulos

Depois de configurar a ponte, você pode iniciar o cabeamento do seu novo sistema.

Sobre esta tarefa

Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).

Passos

1. Encadeie em série as gavetas de disco em cada pilha:

   a. Começando pela primeira gaveta lógica na stack, conecte Iom A porta 3 à IOM A porta 1 à IOM A na próxima gaveta até que cada IOM A na stack seja conectada.

   b. Repita o subpasso anterior para IOM B.

   c. Repita as subetapas anteriores para cada pilha.

   O *Installation and Service Guide* do modelo de compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.

2. Ligue as gavetas de disco e, em seguida, defina as IDs de gaveta.
   - É necessário desligar cada compartimento de disco.
   - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
3. Cable disk shelves to the FibreBridge bridges.

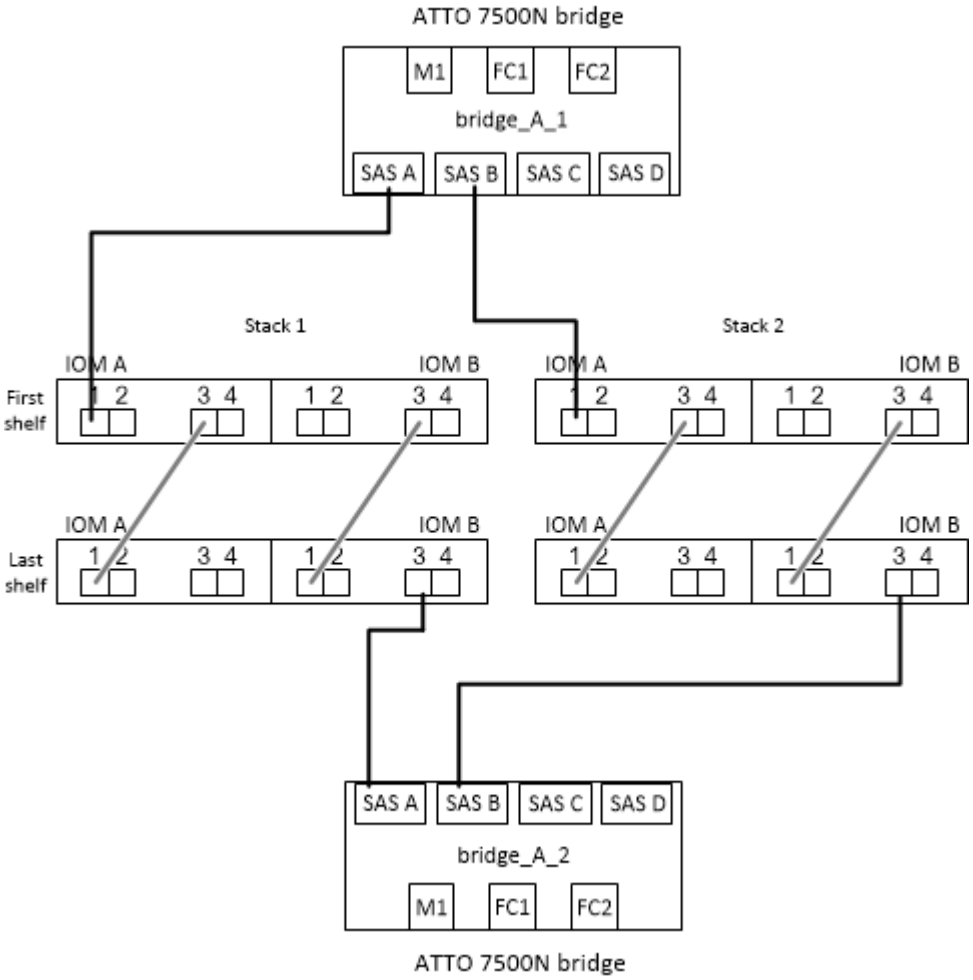
   a. Para a primeira stack de gavetas de disco, cable IOM A da primeira gaveta para a porta SAS a na FibreBridge A e cable IOM B da última gaveta para a porta SAS a na FibreBridge B.

   b. Para stacks de gaveta adicionais, repita a etapa anterior usando a próxima porta SAS disponível nas bridges do FibreBridge, usando a porta B para a segunda stack, a porta C para a terceira stack e a porta D para a quarta stack.

   c. Durante o cabeamento, conete as pilhas baseadas nos módulos IOM12 e IOM3/IOM6 à mesma ponte desde que estejam conetadas a portas SAS separadas.

   > Cada stack pode usar modelos diferentes de IOM, mas todas as gavetas de disco em uma stack precisam usar o mesmo modelo.

A ilustração a seguir mostra as prateleiras de disco conetadas a um par de pontes FibreBridge 7600N ou 7500N:



Faça um cabo de uma ponte FibreBridge 7600N ou 7500N com prateleiras usando módulos IOM6 ou IOM3

Depois de configurar a ponte, você pode iniciar o cabeamento do seu novo sistema. A ponte FibreBridge 7600N ou 7500N usa conetores mini-SAS e suporta prateleiras que usam módulos IOM6 ou IOM3.

Sobre esta tarefa

Os módulos IOM3 não são suportados com bridges FibreBridge 7600N.

Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).

Passos

1. Encadeie as prateleiras em cada pilha.

   a. Para a primeira stack de gavetas, cable IOM Uma porta quadrada da primeira gaveta para a porta SAS A na FibreBridge A.

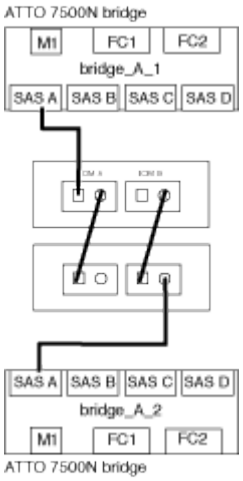
   b. Para a primeira stack de gavetas, a porta circular IOM B do cabo da última gaveta até a porta SAS A no FibreBridge B.

O *Installation and Service Guide* para o modelo de prateleira fornece informações detalhadas sobre

prateleiras de encadeamento em série.

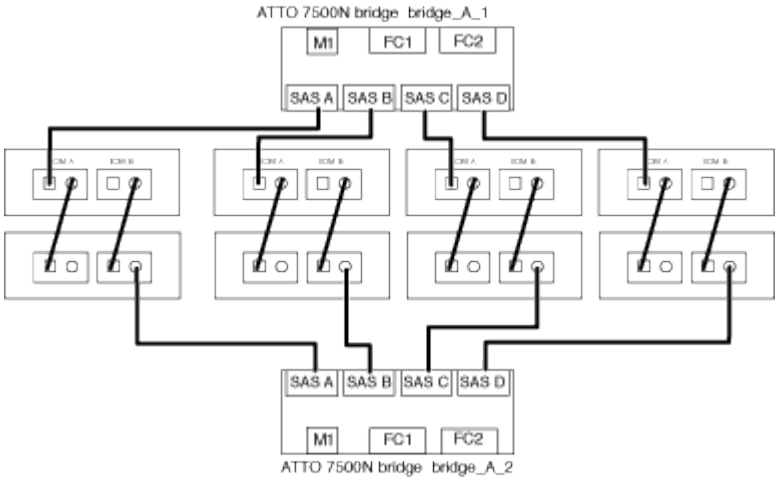
"Guia de instalação e serviço das gavetas de disco SAS para DS4243, DS2246, DS4486 e DS4246"

A ilustração a seguir mostra um conjunto de pontes cabeadas para uma pilha de prateleiras:



2. Para stacks de gaveta adicionais, repita as etapas anteriores usando a próxima porta SAS disponível nas bridges do FibreBridge, usando a porta B para uma segunda stack, a porta C para uma terceira stack e a porta D para uma quarta stack.

   A ilustração a seguir mostra quatro pilhas conetadas a um par de pontes FibreBridge 7600N ou 7500N.



Verifique a conectividade de ponte e faça o cabeamento das pontes FC para SAS às portas FC do controlador

É necessário fazer o cabeamento das pontes às portas FC do controlador em uma configuração MetroCluster conetada a ponte de dois nós.

Passos

1. Verifique se cada bridge pode detetar todas as unidades de disco e prateleiras de disco às quais a ponte está conetada:

   `sastargets`

   O `sastargets` comando output mostra os dispositivos (discos e prateleiras de discos) conetados à ponte. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os

dispositivos.

A saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

2. Verifique se o comando output mostra que a ponte está conetada aos discos e compartimentos de disco corretos na pilha.

Se a saída for…	Então…
Correto	Repita Passo 1 para cada ponte restante.
Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS reabilitando as gavetas de disco nas pontes. Cable disk shelves to the bridges b. Repita Passo 1 para cada ponte restante.

3. Cable cada bridge para as portas FC do controlador:

   a. Cabo FC porta 1 da ponte para uma porta FC no controlador em cluster_A.

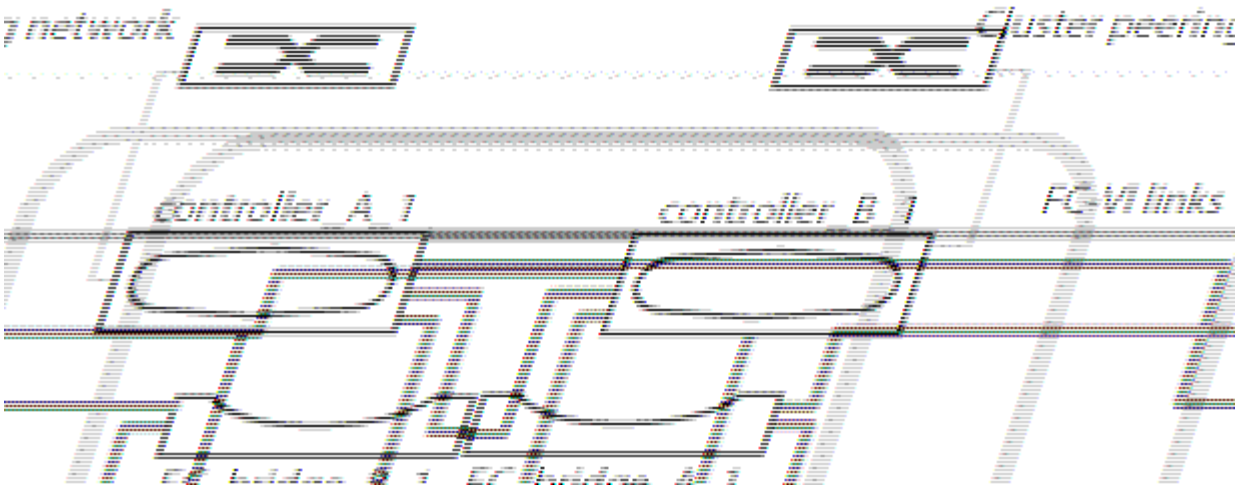
   b. Cabo FC porta 2 da ponte para uma porta FC no controlador em cluster_B.

   - Se o controlador estiver configurado com um adaptador FC de quatro portas, certifique-se de que as bridges em ambas as extremidades da pilha de armazenamento não estejam conetadas a duas portas FC no mesmo ASIC. Por exemplo:
     - O porto a e o porto b compartilham o mesmo ASIC.
     - A porta c e a porta d compartilham o mesmo ASIC.

     Neste exemplo, conete FC_bridge_A_1 à porta a e FC_bridge_A2 à porta c.

   - Se o controlador estiver configurado com mais de um adaptador FC, não faça o cabeamento das pontes de ambas as extremidades da pilha de storage ao mesmo adaptador.

     Nesse cenário, você deve conetar FC_bridge_A_1 a uma porta FC integrada e conetar FC_bridge_A_2 a uma porta FC em um adaptador em um slot de expansão.



4. Repita Passo 3nas outras pontes até que todas as pontes tenham sido cabeadas.

Proteja ou desprenda a ponte FibreBridge

Para desativar facilmente protocolos Ethernet potencialmente inseguros em uma ponte, começando com o ONTAP 9.5, você pode proteger a ponte. Isto desativa as portas Ethernet da ponte. Você também pode reativar o acesso Ethernet.

Sobre esta tarefa

- A proteção da ponte desativa os protocolos e serviços de porta telnet e de outras portas IP (FTP, ExpressNAV, ICMP ou Quicknav) na ponte.
- Este procedimento usa gerenciamento fora da banda usando o prompt ONTAP, que está disponível a partir do ONTAP 9.5.

  Você pode emitir os comandos da CLI de bridge se não estiver usando o gerenciamento fora da banda.

- O `unsecurebridge` comando pode ser usado para reativar as portas Ethernet.
- No ONTAP 9.7 e anteriores, executar o `securebridge` comando no FibreBridge ATTO pode não atualizar o status da ponte corretamente no cluster de parceiros. Se isso ocorrer, execute o `securebridge` comando do cluster de parceiros.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. A partir do prompt ONTAP do cluster que contém a ponte, proteja ou desprenda a ponte.
   - O seguinte comando protege bridge_A_1:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
     ```

   - O comando a seguir desprotege bridge_A_1:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
     ```

2. No prompt ONTAP do cluster que contém a ponte, salve a configuração da ponte:

   ```
   storage bridge run-cli -bridge <bridge-name> -command saveconfiguration
   ```

   O seguinte comando protege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. No prompt ONTAP do cluster que contém a ponte, reinicie o firmware da ponte:

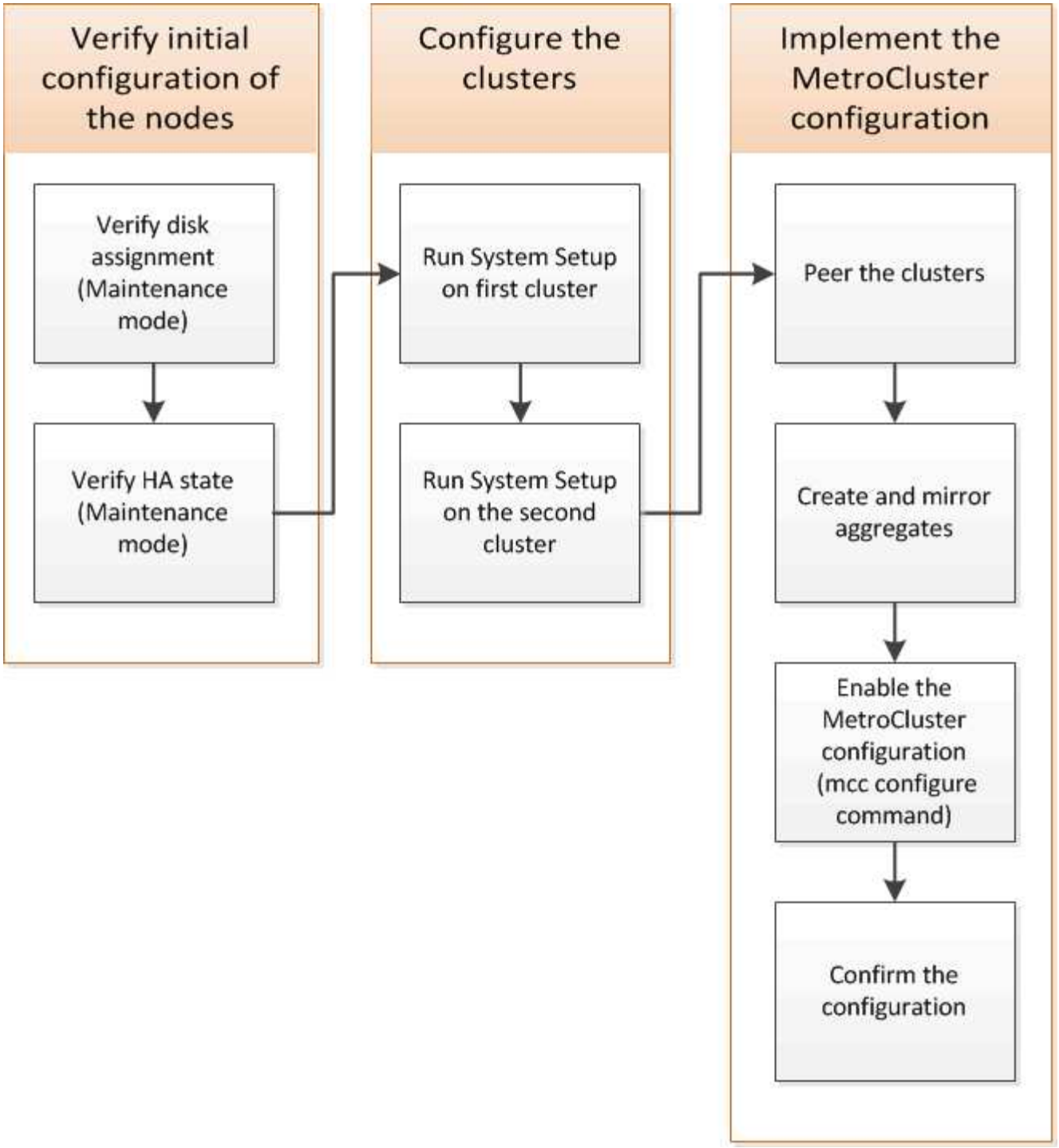
   ```
   storage bridge run-cli -bridge <bridge-name> -command firmwarerestart
   ```

   O seguinte comando protege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
   ```

Configurando o software MetroCluster no ONTAP

É necessário configurar cada nó na configuração do MetroCluster no ONTAP, incluindo as configurações no nível do nó e a configuração dos nós em dois locais. Você também deve implementar a relação MetroCluster entre os dois sites.



Passos

1. Reúna os endereços IP necessários para os módulos do controlador antes de iniciar o processo de configuração.
2. Preencha a Planilha de informações de rede IP para o local A..

Folha de cálculo de informações de rede IP para o local A

Você deve obter endereços IP e outras informações de rede para o primeiro site do MetroCluster (site A) do administrador da rede antes de configurar o sistema.

Site Um cluster de criação de informações

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster. Exemplo usado nesta informação: Site_A	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do site A.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1. Exemplo usado nesta informação: Controller_A_1				
Nó 2. Não é necessário se estiver usando a configuração MetroCluster de dois nós (um nó em cada local). Exemplo usado nesta informação: Controller_A_2				

Crie um site LIFs e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				

Nó 1 IC LIF 2				

Site A informações do servidor de tempo

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local A Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		Anfitriões de correio
Endereços IP ou nomes		Protocolo de transporte
HTTP, HTTPS OU SMTP		Servidor proxy
	Endereços de e-mail do destinatário ou listas de distribuição	Mensagens completas
	Mensagens concisas	

Site A informações do SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção. Isso requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1			

Folha de cálculo de informações de rede IP para o local B.

Você deve obter endereços IP e outras informações de rede para o segundo site da MetroCluster (site B) do administrador da rede antes de configurar o sistema.

Informações sobre a criação do cluster do local B.

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster. Exemplo usado nesta informação: Site_B	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do local B.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1. Exemplo usado nesta informação: Controller_B_1				
Nó 2. Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local). Exemplo usado nesta informação: Controller_B_2				

LIFs do local B e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				
Nó 1 IC LIF 2				

Informações do servidor de hora local B.

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local B Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		Anfitriões de correio
Endereços IP ou nomes		Protocolo de transporte
HTTP, HTTPS OU SMTP		Servidor proxy
	Endereços de e-mail do destinatário ou listas de distribuição	Mensagens completas
	Mensagens concisas	

Local B Informação SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção, o que requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1 (controlador_B_1)			

Semelhanças e diferenças entre configurações padrão de cluster e MetroCluster

A configuração dos nós em cada cluster em uma configuração MetroCluster é semelhante à dos nós em um cluster padrão.

A configuração do MetroCluster é baseada em dois clusters padrão. Fisicamente, a configuração deve ser simétrica, com cada nó tendo a mesma configuração de hardware e todos os componentes do MetroCluster devem ser cabeados e configurados. No entanto, a configuração básica de software para nós em uma configuração MetroCluster é a mesma para nós em um cluster padrão.

Etapa de configuração	Configuração padrão de cluster	Configuração do MetroCluster

Configurar LIFs de gerenciamento, cluster e dados em cada nó.	O mesmo em ambos os tipos de clusters	Configure o agregado raiz.
O mesmo em ambos os tipos de clusters	Configure o cluster em um nó no cluster.	O mesmo em ambos os tipos de clusters
Junte o outro nó ao cluster.	O mesmo em ambos os tipos de clusters	Crie um agregado de raiz espelhado.
Opcional	Obrigatório	Espreite os clusters.
Opcional	Obrigatório	Ative a configuração do MetroCluster.

Restaurando os padrões do sistema e configurando o tipo HBA em um módulo do controlador

Para garantir uma instalação bem-sucedida do MetroCluster, redefina e restaure padrões nos módulos do controlador.

Importante

Essa tarefa só é necessária para configurações Stretch usando bridges FC-para-SAS.

Passos

1. No prompt Loader, retorne as variáveis ambientais à configuração padrão:

   ```
   set-defaults
   ```

2. Inicialize o nó no modo Manutenção e, em seguida, configure as configurações para quaisquer HBAs no sistema:

   a. Arranque no modo de manutenção:

      ```
      boot_ontap maint
      ```

   b. Verifique as definições atuais das portas:

      ```
      ucadmin show
      ```

   c. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter_name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter_name`*
Destino de FC	`fcadmin config -t target` *`adapter_name`*

Iniciador FC	`fcadmin config -t initiator` *`adapter_name`*

3. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

4. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

5. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

6. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

7. Inicialize o nó no menu de inicialização:

   `boot_ontap menu`

   Depois de executar o comando, aguarde até que o menu de inicialização seja exibido.

8. Limpe a configuração do nó digitando "wipeconfig" no prompt do menu de inicialização e pressione Enter.

   A tela a seguir mostra o prompt do menu de inicialização:

```
Please choose one of the following:

     (1) Normal Boot.
     (2) Boot without /etc/rc.
     (3) Change password.
     (4) Clean configuration and initialize all disks.
     (5) Maintenance mode boot.
     (6) Update flash from backup config.
     (7) Install new software first.
     (8) Reboot node.
     (9) Configure Advanced Drive Partitioning.
     Selection (1-9)?  wipeconfig
 This option deletes critical system configuration, including cluster
membership.
 Warning: do not run this option on a HA node that has been taken over.
 Are you sure you want to continue?: yes
 Rebooting to finish wipeconfig request.
```

Configurando portas FC-VI em uma placa quad-port X1132A-R6 em sistemas FAS8020

Se você estiver usando a placa quad-port X1132A-R6 em um sistema FAS8020, você pode entrar no modo de manutenção para configurar as portas 1a e 1b para uso de FC-VI e iniciador. Isso não é necessário nos sistemas MetroCluster recebidos de fábrica, nos quais as portas são definidas adequadamente para sua configuração.

Sobre esta tarefa

Esta tarefa deve ser executada no modo Manutenção.

> ⓘ A conversão de uma porta FC para uma porta FC-VI com o comando uadministrador só é compatível com os sistemas FAS8020 e AFF 8020. A conversão de portas FC para portas FCVI não é compatível em nenhuma outra plataforma.

Passos

1. Desative as portas:

```
storage disable adapter 1a

storage disable adapter 1b
```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Verifique se as portas estão desativadas:

   `ucadmin show`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. Defina as portas a e b para o modo FC-VI:

   `ucadmin modify -adapter 1a -type fcvi`

   O comando define o modo em ambas as portas no par de portas, 1a e 1b (mesmo que apenas 1a seja especificado no comando).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. Confirme se a alteração está pendente:

```
ucadmin show
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Desligue o controlador e reinicie-o no modo de manutenção.
6. Confirme a alteração de configuração:

```
ucadmin show local
```

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

Verificando a atribuição de discos no modo Manutenção em uma configuração de dois nós

Antes de iniciar totalmente o sistema no ONTAP, você pode opcionalmente inicializar o sistema no modo Manutenção e verificar a atribuição de disco nos nós. Os discos devem ser atribuídos para criar uma configuração totalmente simétrica, com os dois locais que possuem suas próprias gavetas de disco e fornecimento de dados, em que cada nó e cada pool têm um número igual de discos espelhados atribuídos a eles.

Antes de começar

O sistema tem de estar no modo de manutenção.

Sobre esta tarefa

Os novos sistemas MetroCluster têm atribuições de disco concluídas antes do envio.

A tabela a seguir mostra exemplos de atribuições de pool para uma configuração do MetroCluster. Os discos são atribuídos a pools por compartimento.

Compartimento de disco (*exemplo nome*)…	No local…	Pertence a…	E é atribuído a esse nó…
Compartimento de disco 1 (shelf_A_1_1)	Local A	Nó A 1	Piscina 0
Compartimento de disco 2 (shelf_A_1_3)	Compartimento de disco 3 (gaveta_B_1_1)	Nó B 1	Piscina 1
Compartimento de disco 4 (gaveta_B_1_3)	Compartimento de disco 9 (gaveta_B_1_2)	Local B	Nó B 1
Piscina 0	Compartimento de disco 10 (gaveta_B_1_4)	Compartimento de disco 11 (shelf_A_1_2)	Nó A 1

Se a configuração incluir DS460C compartimentos de disco, você deve atribuir manualmente os discos usando as seguintes diretrizes para cada gaveta de 12 discos:

Atribuir estes discos na gaveta…	Para este nó e pool…
1 - 6	Pool do nó local 0
7 - 12	Pool do parceiro DR 1

Esse padrão de atribuição de disco minimiza o efeito em um agregado se uma gaveta ficar offline.

Passos

1. Se o seu sistema foi recebido de fábrica, confirme as atribuições de prateleira:

   ```
   disk show –v
   ```

2. Se necessário, você pode atribuir explicitamente discos nas gavetas de disco conetadas ao pool apropriado

   ```
   disk assign
   ```

   Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1. Você deve atribuir um número igual de prateleiras a cada pool.

   a. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.

   b. No nó no local A, atribua sistematicamente as gavetas de disco locais ao pool 0 e às gavetas de disco remotas ao pool 1: Mais
   `disk assign -shelf` *`disk_shelf_name`* `-p` *`pool`*

      Se o nó_A_1 do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

c. No nó do local remoto (local B), atribua sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1: Mais
`disk assign -shelf disk_shelf_name -p pool`

Se o nó_B_1 do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf shelf_B_1_2   -p 0
*> disk assign -shelf shelf_B_1_4  -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
 *> disk assign -shelf shelf_B_1_3 -p 1
```

a. Mostrar as IDs e os compartimentos do compartimento de disco para cada disco
`disk show –v`

Verificando o estado de HA dos componentes

Em uma configuração Stretch MetroCluster que não está pré-configurada na fábrica, você deve verificar se o estado HA do controlador e do componente do chassi está definido como "mcc-2n" para que eles iniciem corretamente. Para sistemas recebidos de fábrica, esse valor é pré-configurado e você não precisa verificá-lo.

Antes de começar

O sistema tem de estar no modo de manutenção.

Passos

1. No modo de manutenção, visualize o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O módulo do controlador e o chassi devem mostrar o valor "mcc-2n".

2. Se o estado do sistema exibido do controlador não for "mcc-2n", defina o estado HA para o controlador:

   `ha-config modify controller mcc-2n`

3. Se o estado do sistema exibido do chassi não for "mcc-2n", defina o estado HA para o chassi:

   `ha-config modify chassis mcc-2n`

   Parar o nó.

   Aguarde até que o nó volte ao prompt DO Loader.

4. Repita estas etapas em cada nó na configuração do MetroCluster.

Configurando o ONTAP em uma configuração de MetroCluster de dois nós

Em uma configuração de MetroCluster de dois nós, em cada cluster, você deve inicializar o nó, sair do assistente de configuração de cluster e usar o `cluster setup` comando para configurar o nó em um cluster de nó único.

Antes de começar

Você não deve ter configurado o processador de serviço.

Sobre esta tarefa

Essa tarefa é para configurações de MetroCluster de dois nós que usam storage nativo do NetApp.

Essa tarefa deve ser executada em ambos os clusters na configuração do MetroCluster.

Para obter mais informações gerais sobre a configuração do ONTAP, consulte a. "Configuração do ONTAP"

Passos

1. Ligue o primeiro nó.

   Repita esta etapa no nó no local de recuperação de desastres (DR).

   O nó é inicializado e, em seguida, o assistente de Configuração de cluster é iniciado no console informando que o AutoSupport será ativado automaticamente.

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

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



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

2. Criar um novo cluster:

   ```
   create
   ```

3. Escolha se o nó deve ser usado como um cluster de nó único.

   ```
   Do you intend for this node to be used as a single node cluster? {yes,
   no} [yes]:
   ```

4. Aceite o padrão do sistema "sim" pressionando Enter, ou insira seus próprios valores digitando "não" e,

em seguida, pressionando Enter.

5. Siga as instruções para concluir o assistente **Configuração de cluster**, pressione Enter para aceitar os valores padrão ou digitar seus próprios valores e pressione Enter.

   Os valores padrão são determinados automaticamente com base na sua plataforma e configuração de rede.

6. Depois de concluir o assistente **Cluster Setup** e ele sair, verifique se o cluster está ativo e se o primeiro nó está em bom estado:

   `cluster show`

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

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

   Se for necessário alterar qualquer uma das configurações inseridas para o SVM admin ou nó SVM, você poderá acessar o assistente **Configuração de cluster** usando o `cluster setup` comando.

Configuração dos clusters em uma configuração do MetroCluster

É necessário fazer peer nos clusters, espelhar os agregados raiz, criar um agregado de dados espelhados e, em seguida, emitir o comando para implementar as operações do MetroCluster.

Peering dos clusters

Os clusters na configuração do MetroCluster precisam estar em um relacionamento de mesmo nível para que possam se comunicar uns com os outros e executar o espelhamento de dados essencial para a recuperação de desastres do MetroCluster.

Informações relacionadas

"Configuração expressa de peering de cluster e SVM"

"Considerações ao usar portas dedicadas"

"Considerações ao compartilhar portas de dados"

Configurando LIFs entre clusters

É necessário criar LIFs entre clusters nas portas usadas para comunicação entre os clusters de parceiros da MetroCluster. Você pode usar portas dedicadas ou portas que também têm tráfego de dados.

Configurando LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede em "'cluster01"":

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que os portos "'e0e'" e "'e0f'" não foram atribuídos LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port

Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   O exemplo a seguir atribui as portas "'e0e"" e "'e0f" ao grupo de failover "'intercluster01" no SVM do sistema "'cluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

   `network interface failover-groups show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`
ONTAP 9 F.5 e anteriores	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "'cluster01_icl01" e "'cluster01_icl02" no grupo de failover "'intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface show -service-policy default-intercluster`
ONTAP 9 F.5 e anteriores	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verifique se as LIFs entre clusters são redundantes:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface show -service-policy default-intercluster -failover`

Em ONTAP 9.5 e anteriores	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "'cluster01_icl01" e "'cluster01_icl02" na porta SVM "'e0e" falharão para a porta "'e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Informações relacionadas

"Considerações ao usar portas dedicadas"

Configurando LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede em "'cluster01"":

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Criar LIFs entre clusters no sistema:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface create -vserver` *system_SVM* `-lif` *LIF_name* `-service-policy default-intercluster -home -node node -home-port` *port* `-address` *port_IP* `-netmask` *netmask*
ONTAP 9 F.5 e anteriores	`network interface create -vserver` *system_SVM* `-lif` *LIF_name* `-role intercluster -home-node` *node* `-home-port` *port* `-address` *port_IP* `-netmask` *netmask*

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "'cluster01_icl01" e "'cluster01_icl02":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface show -service-policy default-intercluster`
ONTAP 9 F.5 e anteriores	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	`network interface show –service-policy default-intercluster -failover`
ONTAP 9 F.5 e anteriores	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "'cluster01_icl01" e "'cluster01_icl02" na porta "'e0c" falharão para a porta "'e0d".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Informações relacionadas

"Considerações ao compartilhar portas de dados"

Criando um relacionamento de cluster peer

É necessário criar o relacionamento de peers de clusters entre os clusters do MetroCluster.

Criando um relacionamento de cluster peer

Você pode usar o `cluster peer create` comando para criar uma relação entre pares entre um cluster local e remoto. Após a criação da relação de pares, você pode executar `cluster peer create` no cluster remoto para autenticá-la no cluster local.

Antes de começar

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior.

Passos

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

   `cluster peer create -generate-passphrase -offer-expiration` *`MM/DD/YYYY HH:MM:SS`*`|1…7days|1…168hours -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Se você especificar ambos `-generate-passphrase` e `-peer-addrs`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addrs` poderá usar a senha gerada.

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um relacionamento de peer de cluster em um cluster remoto não especificado:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. No cluster de origem, autentique o cluster de origem no cluster de destino:

   `cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autentica o cluster local para o cluster remoto nos endereços IP 192.140.112.101 e 192.140.112.102 do LIF:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Criando um relacionamento de cluster peer (ONTAP 9.2 e anterior)

Você pode usar o `cluster peer create` comando para iniciar uma solicitação de um relacionamento de peering entre um cluster local e remoto. Depois que o relacionamento de pares tiver sido solicitado pelo

cluster local, você pode executar `cluster peer create` no cluster remoto para aceitar o relacionamento.

Antes de começar

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os administradores de cluster devem ter concordado com a frase-passe que cada cluster usará para se autenticar com o outro.

Passos

1. No cluster de destino de proteção de dados, crie uma relação de mesmo nível com o cluster de origem de proteção de dados:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria uma relação de peer de cluster com o cluster remoto nos endereços IP de LIF 192.168.2.201 e 192.168.2.202:

   ```
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   Digite a senha para o relacionamento de pares quando solicitado.

2. No cluster de origem de proteção de dados, autentique o cluster de origem no cluster de destino:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autentica o cluster local para o cluster remoto nos endereços IP 192.140.112.203 e 192.140.112.204 do LIF:

   ```
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

   `cluster peer show –instance`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

   `cluster peer health show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Espelhamento dos agregados de raiz

É necessário espelhar os agregados raiz para fornecer proteção de dados.

Sobre esta tarefa

Por padrão, o agregado raiz é criado como agregado do tipo RAID-DP. Você pode alterar o agregado raiz de RAID-DP para o agregado do tipo RAID4. O comando a seguir modifica o agregado raiz para o agregado do tipo RAID4:

`storage aggregate modify -aggregate *aggr_name* -raidtype raid4`

Em sistemas que não sejam ADP, o tipo RAID do agregado pode ser modificado do RAID-DP padrão para RAID4 antes ou depois que o agregado é espelhado.

Passos

1. Espelhar o agregado raiz:

   `storage aggregate mirror aggr_name`

   O comando a seguir espelha o agregado raiz para "'controller_A_1":

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Isso reflete o agregado, por isso consiste em um Plex local e um Plex remoto localizado no local remoto de MetroCluster.

2. Repita a etapa anterior para cada nó na configuração do MetroCluster.

Informações relacionadas

"Gerenciamento de storage lógico"

"Conceitos de ONTAP"

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

Antes de começar

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.

Sobre esta tarefa

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.

  "Gerenciamento de disco e agregado"

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   `storage disk show -spare -owner node_name`

2. Criar o agregado:

   `storage aggregate create -mirror true`

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado

em qualquer nó do cluster. Para garantir que o agregado seja criado em um nó específico, use o `-node` parâmetro ou especifique as unidades que são de propriedade desse nó.

Você pode especificar as seguintes opções:

- Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
- Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
- Número de unidades a incluir

> Na configuração mínima suportada, na qual um número limitado de unidades está disponível, você deve usar a opção force-small-Aggregate para permitir a criação de um agregado RAID-DP de três discos.

- Estilo de checksum para usar para o agregado
- Tipo de unidades a utilizar
- Tamanho das unidades a utilizar
- Velocidade de condução a utilizar
- Tipo RAID para grupos RAID no agregado
- Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
- Se unidades com RPM diferentes são permitidas para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Criação de agregados de dados sem espelhamento

Você pode, opcionalmente, criar agregados de dados sem espelhamento para dados que não exigem o espelhamento redundante fornecido pelas configurações do MetroCluster.

Antes de começar

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode verificar se o tipo de unidade correto está selecionado.

Exemplo 1. Sobre esta tarefa

ATENÇÃO: Nas configurações MetroCluster FC, os agregados sem espelhamento só estarão online após um switchover se os discos remotos no agregado estiverem acessíveis. Se os ISLs falharem, o nó local poderá não conseguir aceder aos dados nos discos remotos sem espelhamento. A falha de um agregado pode levar a uma reinicialização do nó local.

Os agregados sem espelhamento devem ser locais para o nó que os possui.

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.
- O "Gerenciamento de discos e agregados" contém mais informações sobre o espelhamento de agregados.

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   `storage disk show -spare -owner` *`node_name`*

2. Criar o agregado:

   `storage aggregate create`

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para verificar se o agregado é criado em um nó específico, você deve usar o `-node` parâmetro ou especificar unidades que são de propriedade desse nó.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
   - Número de unidades a incluir
   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
   - Se unidades com RPM diferentes são permitidas para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

     O comando a seguir cria um agregado sem espelhamento com 10 discos:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Implementando a configuração do MetroCluster

Você deve executar o `metrocluster configure` comando para iniciar a proteção de dados em uma configuração do MetroCluster.

Antes de começar

- Deve haver pelo menos dois agregados de dados espelhados não-raiz em cada cluster.

  Agregados de dados adicionais podem ser espelhados ou sem espelhamento.

  Verifique os tipos de agregados:

  `storage aggregate show`

  > Se você quiser usar um único agregado de dados espelhados, consulte "Configurar o software MCC no ONTAP" para obter instruções.

- O estado ha-config dos controladores e chassis deve ser "mcc-2n".

Sobre esta tarefa

Você pode emitir o `metrocluster configure` comando uma vez, em qualquer um dos nós, para ativar a configuração do MetroCluster. Você não precisa emitir o comando em cada um dos sites ou nós, e não importa em qual nó ou site você escolher emitir o comando.

Passos

1. Configure o MetroCluster no seguinte formato:

Se a sua configuração do MetroCluster tiver…	Então faça isso…
Vários agregados de dados	A partir do prompt de qualquer nó, configure o MetroCluster: `metrocluster configure` *`node-name`*

Um único agregado de dados espelhados	a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado: `set -privilege advanced` Você precisa responder com "'y'" quando for solicitado a continuar para o modo avançado e você vir o prompt do modo avançado (*>). b. Configure o MetroCluster com o `-allow-with-one-aggregate true` parâmetro: `metrocluster configure -allow-with-one-aggregate true` *`node-name`* c. Voltar para o nível de privilégio de administrador `set -privilege admin`

> A prática recomendada é ter vários agregados de dados. Se o primeiro grupo de DR tiver apenas um agregado e quiser adicionar um grupo de DR com um agregado, mova o volume de metadados do agregado de dados único. Para obter mais informações sobre este procedimento, "Movimentação de um volume de metadados nas configurações do MetroCluster"consulte .

O comando a seguir habilita a configuração do MetroCluster em todos os nós do grupo DR que contém "'controller_A_1":

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verifique o status da rede no local A:

   `network port show`

   O exemplo a seguir mostra o uso da porta de rede:

```
cluster_A::> network port show
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000

7 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.

   a. Verifique a configuração a partir do site A
   `metrocluster show`

   ```
   cluster_A::> metrocluster show

   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-
   disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-
   disaster
   ```

   b. Verifique a configuração a partir do local B
   `metrocluster show`

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

Configuração de pontes FC para SAS para monitoramento de integridade

Em sistemas que executam versões do ONTAP anteriores a 9,8, se sua configuração incluir pontes FC para SAS, você deverá executar algumas etapas especiais de configuração para monitorar as pontes FC para SAS na configuração do MetroCluster.

- Ferramentas de monitoramento SNMP de terceiros não são suportadas para bridges FibreBridge.
- A partir do ONTAP 9.8, as bridges FC para SAS são monitoradas por meio de conexões na banda por padrão, e não é necessária configuração adicional.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

   a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
ONTAP 9 F.5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
ONTAP 9 .4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   b. Verifique se a ponte foi adicionada e está configurada corretamente:

      `storage bridge show`

      Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de saúde do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente. Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster. Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Os comandos subsequentes `metrocluster check show` não mostram a saída esperada.

1. Verificar a configuração:

   `metrocluster check run`

   O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Apresentar resultados mais detalhados:

   `metrocluster check run`

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`

   `metrocluster check node show`

   Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

   O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
```

```
ok
                                                    ownership-state
ok
                      controller_A_1_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

O exemplo a seguir mostra a `metrocluster check cluster show` saída do comando para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

Informações relacionadas

"Gerenciamento de disco e agregado"

"Gerenciamento de rede e LIF"

Verificando erros de configuração do MetroCluster com o Config Advisor

Você pode acessar o site de suporte da NetApp e baixar a ferramenta Config Advisor para verificar se há erros de configuração comuns.

O Config Advisor é uma ferramenta de validação de configuração e verificação de integridade. Você pode implantá-lo em sites seguros e sites não seguros para coleta de dados e análise do sistema.

O suporte para Config Advisor é limitado e está disponível apenas online.

1. Vá para a página de download do Config Advisor e baixe a ferramenta.

   "NetApp Downloads: Config Advisor"

2. Execute o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Verificando switchover, cura e switchback

Você deve verificar as operações de switchover, recuperação e switchback da configuração do MetroCluster.

1. Use os procedimentos para comutação negociada, cura e switchback que são mencionados no "Execute switchover, cura e switchback".

Protegendo arquivos de backup de configuração

Você pode fornecer proteção adicional para os arquivos de backup de configuração de cluster especificando um URL remoto (HTTP ou FTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster local.

1. Defina o URL do destino remoto para os arquivos de backup de configuração:

   ```
   system configuration backup settings modify URL-of-destination
   ```

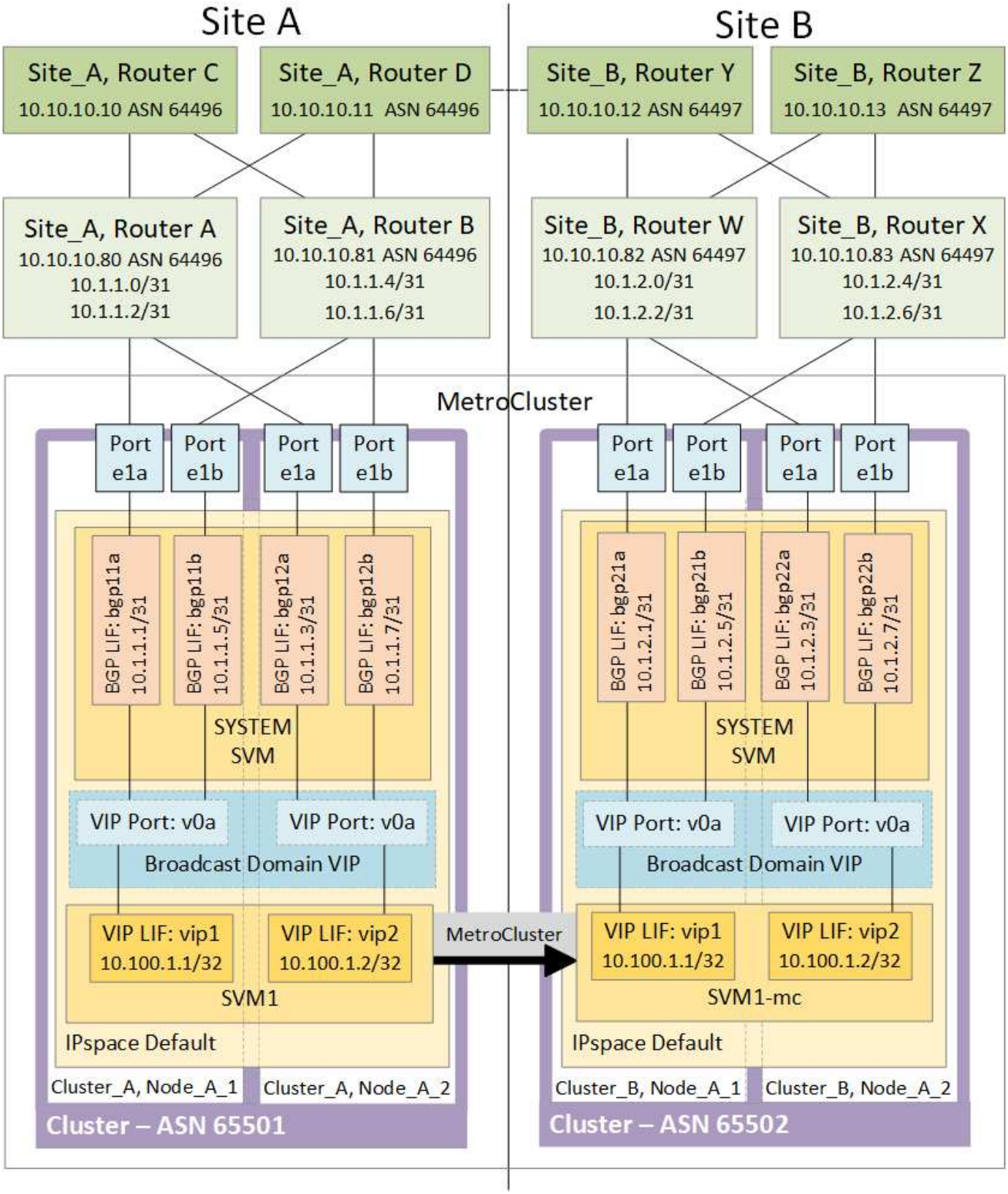
   O "Gerenciamento de clusters com a CLI" contém informações adicionais na seção *Gerenciando backups de configuração*.

Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster

A partir do ONTAP 9.5, o ONTAP oferece suporte à conetividade da camada 3 usando IP virtual (VIP) e protocolo de gateway de borda (BGP). A combinação VIP e BGP para redundância na rede front-end com a redundância MetroCluster back-end fornece uma solução de recuperação de desastres de camada 3.

Revise as diretrizes e a ilustração a seguir ao Planejar sua solução de camada 3. Para obter detalhes sobre como implementar o VIP e o BGP no ONTAP, consulte a seguinte seção:

"Configurando LIFs de IP virtual (VIP)"



Limitações do ONTAP

O ONTAP não verifica automaticamente se todos os nós em ambos os sites da configuração do MetroCluster estão configurados com peering BGP.

O ONTAP não executa agregação de rotas, mas anuncia todos os IPs de LIF virtuais individuais como rotas

de host exclusivas em todos os momentos.

O ONTAP não suporta True anycast — apenas um único nó no cluster apresenta um IP de LIF virtual específico (mas é aceito por todas as interfaces físicas, independentemente de serem LIFs BGP, desde que a porta física faça parte do espaço IPspace correto). Diferentes LIFs podem migrar independentemente um do outro para diferentes nós de hospedagem.

Diretrizes para usar esta solução de camada 3 com uma configuração MetroCluster

Você deve configurar seu BGP e VIP corretamente para fornecer a redundância necessária.

Cenários de implantação mais simples são preferidos em relação a arquiteturas mais complexas (por exemplo, um roteador de peering BGP é acessível em um roteador intermediário não BGP). No entanto, o ONTAP não aplica restrições de design ou topologia de rede.

Os LIFs VIP cobrem apenas a rede frontend/data.

Dependendo da sua versão do ONTAP, você deve configurar LIFs de peering BGP no nó SVM, não no sistema ou na SVM de dados. No ONTAP 9.8, as LIFs de BGP são visíveis no SVM do cluster (sistema) e as SVMs de nó não estão mais presentes.

Cada SVM de dados requer a configuração de todos os endereços potenciais de gateway de primeiro salto (normalmente, o endereço IP de peering do roteador BGP), de modo que o caminho de dados de retorno esteja disponível se ocorrer uma migração de LIF ou failover de MetroCluster.

As LIFs BGP são específicas de nós, semelhantes às LIFs entre clusters - cada nó tem uma configuração exclusiva, que não precisa ser replicado para os nós do local de DR.

A existência do v0a (v0b e assim por diante) valida continuamente a conetividade, garantindo que uma migração de LIF ou failover seja bem-sucedida (ao contrário do L2, onde uma configuração quebrada só é visível após a interrupção).

Uma grande diferença de arquitetura é que os clientes não devem mais compartilhar a mesma sub-rede IP que o VIP de SVMs de dados. Um roteador L3 com recursos apropriados de resiliência e redundância de nível empresarial habilitados (por exemplo, VRRP/HSRP) deve estar no caminho entre o armazenamento e os clientes para que o VIP funcione corretamente.

O processo de atualização confiável do BGP permite migrações de LIF mais suaves, pois elas são marginalmente mais rápidas e têm menor chance de interrupção para alguns clientes.

Você pode configurar o BGP para detetar algumas classes de comportamentos incorretos de rede ou switch mais rápido do que o LACP, se configurado de acordo.

O BGP externo (EBGP) usa números diferentes entre nós ONTAP e roteadores de peering e é a implantação preferida para facilitar a agregação e redistribuição de rotas nos roteadores. O BGP interno (IBGP) e o uso de refletores de rota não são impossíveis, mas fora do escopo de uma configuração VIP direta.

Após a implantação, você deve verificar se o SVM de dados está acessível quando o LIF virtual associado é migrado entre todos os nós em cada local (incluindo switchover de MetroCluster) para verificar a configuração correta das rotas estáticas para o mesmo SVM de dados.

O VIP funciona para a maioria dos protocolos baseados em IP (NFS, SMB, iSCSI).

Testando a configuração do MetroCluster

Você pode testar cenários de falha para confirmar o funcionamento correto da configuração do MetroCluster.

Verificando o switchover negociado

Você pode testar uma operação de switchover negociado (planejada) para confirmar a disponibilidade de dados ininterrupta.

Este teste valida que a disponibilidade de dados não é afetada (exceto para os protocolos SMB (Server Message Block) da Microsoft e Fibre Channel do Solaris), alternando o cluster para o segundo data center.

Este teste deve levar cerca de 30 minutos.

Este procedimento tem os seguintes resultados esperados:

- O `metrocluster switchover` comando apresentará um prompt de aviso.

  Se você responder **`yes`** ao prompt, o site do qual o comando é emitido mudará para o site do parceiro.

Para configurações IP do MetroCluster:

- Para o ONTAP 9.4 e versões anteriores:
  - Os agregados espelhados ficarão degradados após o switchover negociado.
- Para o ONTAP 9.5 e posterior:
  - Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
  - Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Para o ONTAP 9.8 e posterior:
  - Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

Passos

1. Confirme se todos os nós estão no estado configurado e no modo normal:

   `metrocluster node show`

   ```
   cluster_A::>  metrocluster node show

   Cluster                     Configuration State    Mode
   --------------------------- ---------------------
   ------------------------
    Local: cluster_A              configured             normal
   Remote: cluster_B              configured             normal
   ```

2. Inicie a operação de comutação:

`metrocluster switchover`

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Confirme se o cluster local está no estado configurado e no modo de comutação:

`metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. Confirme se a operação de comutação foi bem-sucedida:

`metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Use os `vserver show` comandos e `network interface show` para verificar se as SVMs e LIFs de DR estão online.

Verificando a cura e a troca manual

Você pode testar as operações de reparo e switchback manual para verificar se a disponibilidade de dados não é afetada (exceto para configurações SMB e Solaris FC), alternando o cluster para o data center original após um switchover negociado.

Este teste deve levar cerca de 30 minutos.

O resultado esperado deste procedimento é que os serviços devem ser reenviados para os seus nós domésticos.

Passos

1. Verifique se a cicatrização está concluída:

   `metrocluster node show`

   O exemplo a seguir mostra a conclusão bem-sucedida do comando:

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   heal roots
completed
      cluster_B
              node_B_2         unreachable    -         switched over
42 entries were displayed.metrocluster operation show
```

2. Verifique se todos os agregados são `mirrored`:

   `storage aggregate show`

   O exemplo a seguir mostra que todos os agregados têm um status RAID espelhado:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. Nós de inicialização no local do desastre.
4. Verifique o status da recuperação de switchback:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
            node_A_1            configured     enabled   heal roots
completed
      cluster_B
            node_B_2            configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

5. Execute o interrutor de retorno:

   `metrocluster switchback`

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

6. Confirme o status dos nós:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   normal
      cluster_B
              node_B_2         configured     enabled   normal

2 entries were displayed.
```

7. Confirme o estado:

   `metrocluster operation show`

   A saída deve mostrar um estado bem-sucedido.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Perda de uma única ponte FC para SAS

Você pode testar a falha de uma única ponte FC para SAS para garantir que não haja um ponto único de falha.

Este teste deve levar cerca de 15 minutos.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados quando a ponte é desligada.
- Nenhum failover ou perda de serviço deve ocorrer.
- Apenas um caminho do módulo do controlador para as unidades atrás da ponte está disponível.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Desligue as fontes de alimentação da ponte.
2. Confirme se a monitorização da ponte indica um erro:

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                                    Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
   Status
   ---------- ------------- ------- --------- ---------------- ---------
   -------
   ATTO_10.65.57.145
            bridge_A_1    Atto    FibreBridge 6500N
                                              200000108662d46c true
   error
   ```

3. Confirme se as unidades atrás da ponte estão disponíveis com um único caminho:

   `storage disk error show`

```
cluster_A::> storage disk error show
Disk             Error Type        Error Text
---------------- -----------------
-------------------------------------------
1.0.0            onedomain         1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1            onedomain         1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2            onedomain         1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23           onedomain         1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

Verificação da operação após interrupção da linha elétrica

Você pode testar a resposta da configuração do MetroCluster à falha de uma PDU.

A prática recomendada é que cada unidade de fonte de alimentação (PSU) de um componente seja conetada a uma fonte de alimentação separada. Se ambas as PSUs estiverem conetadas à mesma unidade de distribuição de energia (PDU) e ocorrer uma interrupção elétrica, o local pode ficar inativo e um compartimento completo pode ficar indisponível. A falha de uma linha de alimentação é testada para confirmar que não há incompatibilidade de cabeamento que possa causar uma interrupção do serviço.

Este teste deve levar cerca de 15 minutos.

Este teste requer a desativação da energia de todas as PDUs do lado esquerdo e, em seguida, de todas as PDUs do lado direito em todos os racks que contêm os componentes do MetroCluster.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados à medida que as PDUs são desconetadas.
- Nenhum failover ou perda de serviço deve ocorrer.

Passos

1. Desligue a alimentação das PDUs no lado esquerdo do rack que contém os componentes MetroCluster.
2. Monitore o resultado no console usando os `system environment sensors show -state fault` comandos e. `storage shelf show -errors`

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- -------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Ligue a alimentação novamente para as PDUs do lado esquerdo.
4. Certifique-se de que o ONTAP limpa a condição de erro.
5. Repita os passos anteriores com as PDUs do lado direito.

Verificação da operação após a perda de uma única prateleira de armazenamento

Você pode testar a falha de um único compartimento de storage para verificar se não há um ponto único de falha.

Este procedimento tem os seguintes resultados esperados:

- Uma mensagem de erro deve ser comunicada pelo software de monitorização.
- Nenhum failover ou perda de serviço deve ocorrer.
- A ressincronização do espelho é iniciada automaticamente após a restauração da falha de hardware.

Passos

1. Verifique o status de failover de armazenamento:

```
storage failover show
```

```
cluster_A::> storage failover show

Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       true     Connected to node_A_2
node_A_2       node_A_1       true     Connected to node_A_1
2 entries were displayed.
```

2. Verifique o status agregado:

```
storage aggregate show
```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Verifique se todas as SVMs e volumes de dados estão on-line e fornecendo dados:

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identifique um compartimento no pool 1 para o nó node_A_2 desligar para simular uma falha repentina de hardware:

   `storage aggregate show -r -node node-name !*root`

   O compartimento selecionado deve conter unidades que fazem parte de um agregado de dados espelhados.

   No exemplo a seguir, o ID do compartimento 31 é selecionado para falhar.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                      0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                      1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                      1   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     1.31.3                        1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                        1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.5                        1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                         Pool Type     RPM     Size
Size Status
     -------- ---------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                        0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                        0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                        0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Desligue fisicamente a prateleira selecionada.
6. Verifique novamente o status do agregado:

   `storage aggregate`

   `storage aggregate show -r -node node_A_2 !*root`

   O agregado com unidades no compartimento desligado deve ter um status RAID "desclassificado" e as unidades no Plex afetado devem ter um status de "falha", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
```

```
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
```

```
     dparity  2.30.3                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                     -   -          -  827.7GB
-  (failed)
     parity   FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                    0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     parity   2.30.22                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                    0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Verifique se os dados estão sendo fornecidos e se todos os volumes ainda estão online:

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Ligue fisicamente a prateleira.

   A ressincronização é iniciada automaticamente.

9. Verifique se a ressincronização foi iniciada:

   `storage aggregate show`

   O agregado afetado deve ter um status RAID "resincronizando", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1_root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

resyncing
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

10. Monitore o agregado para confirmar que a ressincronização está concluída:

    `storage aggregate show`

    O agregado afetado deve ter um status RAID "normal", como mostrado no exemplo a seguir:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Conexões em configurações Stretch MetroCluster com LUNs de array

Conexões em configurações Stretch MetroCluster com LUNs de array

Em uma configuração Stretch MetroCluster, com LUNs de array, você precisa conectar as portas FC-VI entre controladores. Há suporte para conectividade direta entre os controladores e os storage arrays e-Series. Para todos os outros arrays de configurações

de LUN, você deve usar switches FC na configuração.

Você também pode configurar uma configuração Stretch MetroCluster com discos e LUNs de array. Em tal configuração, você precisa usar pontes FC para SAS ou cabos óticos SAS para conectar controladores a discos.

Exemplo de uma configuração Stretch MetroCluster com LUNs de array

Em uma configuração Stretch MetroCluster com LUNs de array, você precisa fazer o cabeamento das portas FC-VI para conectividade direta entre os controladores. Além disso, você deve fazer o cabeamento de cada porta HBA do controlador para alternar as portas nos switches FC correspondentes. O cabeamento das LUNs de array é igual ao de uma MetroCluster conectada à malha, com exceção das LUNs de array e-Series, que podem ser conectadas diretamente.

A ilustração a seguir mostra as portas FC-VI cabeadas entre os controladores A e B em uma configuração Stretch MetroCluster:

Os módulos dos controladores de sistemas de storage da FAS9000 usam quatro portas FC-VI cada uma.

Para configurações com LUNs de array e-Series, é possível conectar diretamente aos LUNs e-Series.

"Suporte de conexão direta para configuração Stretch MetroCluster com array NetApp e-Series"

Com exceção da conexão das portas FC-VI, o restante deste procedimento é para a configuração de uma configuração MetroCluster com LUNs de array, que não estejam usando LUNs de array e-Series. Isso requer switches FC que são iguais ao uso de LUNs de array em configurações conectadas à malha.

"Instalação e configuração do MetroCluster conectado à malha"

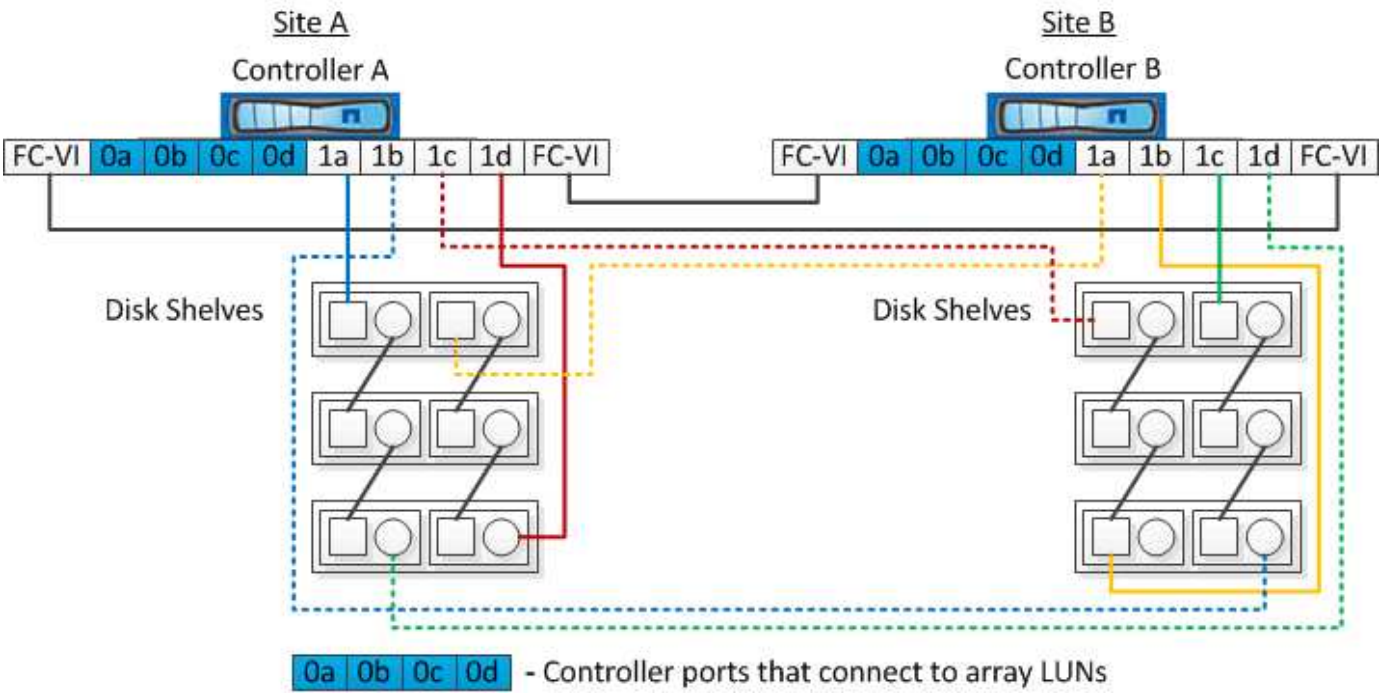
Exemplos de configurações Stretch MetroCluster de dois nós com discos e LUNs de array

Para configurar uma configuração Stretch MetroCluster com discos nativos e LUNs de array, você precisa usar pontes FC para SAS ou cabos óticos SAS para conectar os sistemas ONTAP às gavetas de disco. Além disso, os switches FC devem ser usados para conectar LUNs de array aos sistemas ONTAP.

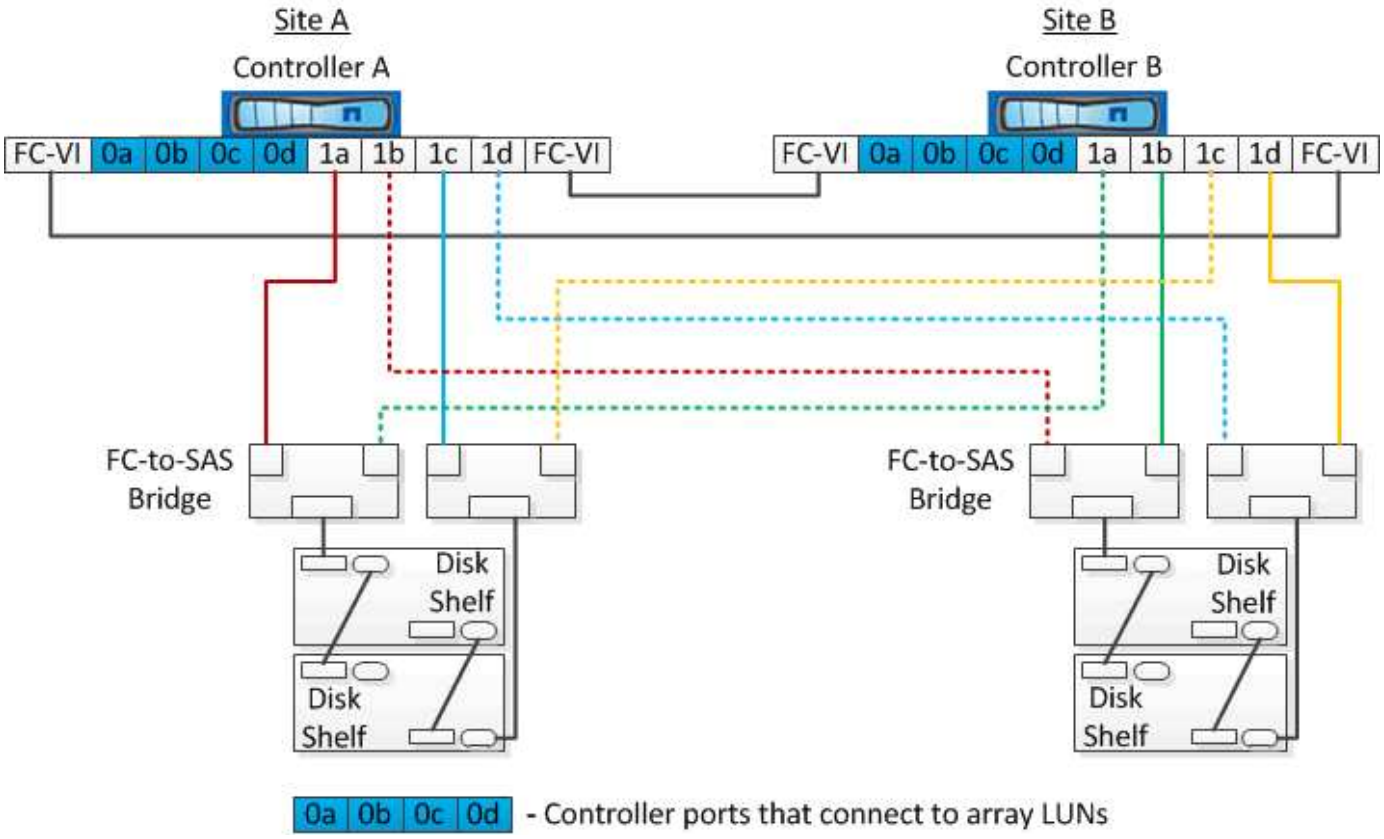
É necessário um mínimo de oito portas HBA para que um sistema ONTAP se conete a discos nativos e LUNs de storage.

Nos exemplos a seguir que representam configurações de MetroCluster alongadas de dois nós com discos e LUNs de array, as portas HBA de 0a a 0d são usadas para conexão com LUNs de array. As portas HBA 1a a 1D são usadas para conexões com discos nativos.

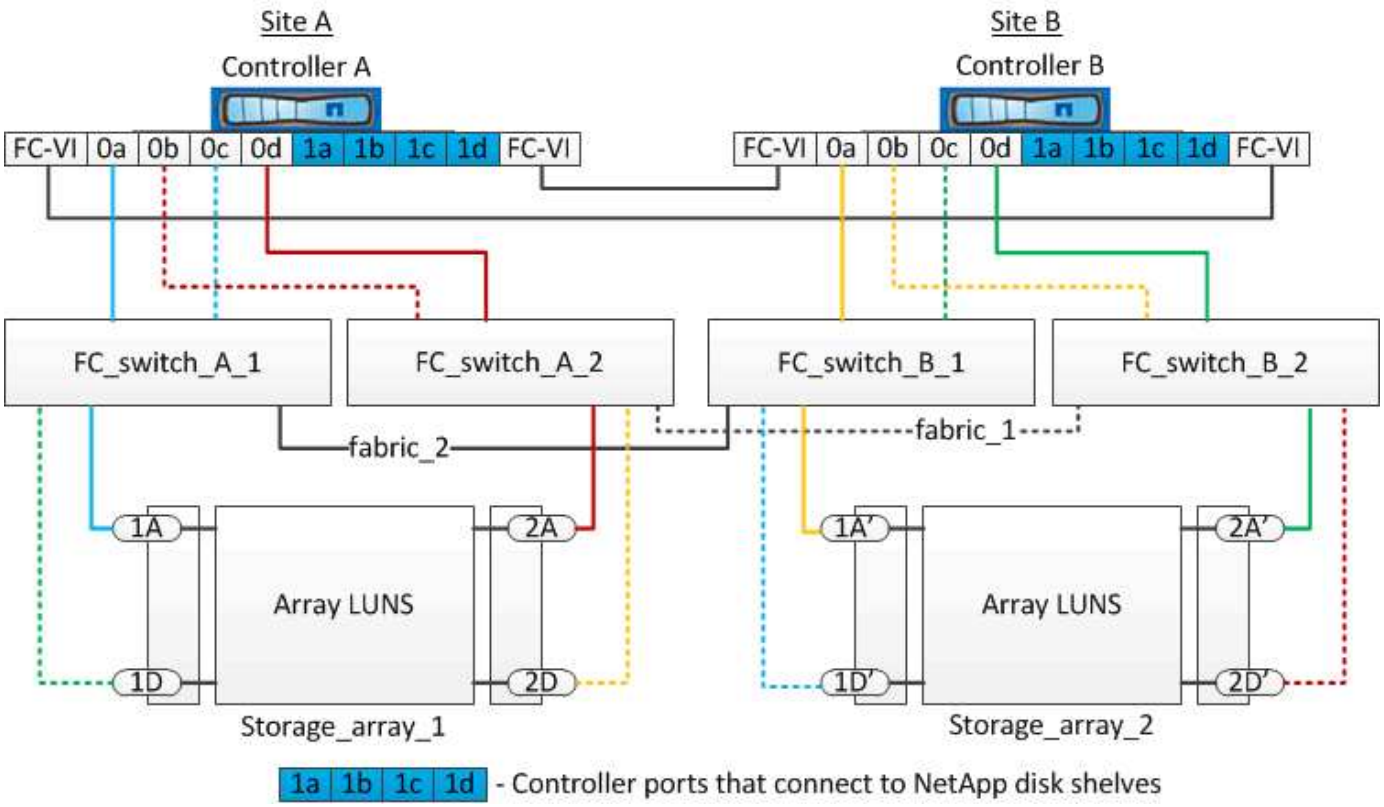
A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós na qual os discos nativos são conetados aos sistemas ONTAP usando cabos óticos SAS:



A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós na qual os discos nativos são conetados aos sistemas ONTAP usando bridges FC-para-SAS:



A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós com as conexões LUN de array:



Se necessário, você também pode usar os mesmos switches FC para conectar discos nativos e LUNs de array às controladoras na configuração MetroCluster.

"Instalação e configuração do MetroCluster conectado à malha"

Exemplo de uma configuração Stretch MetroCluster com storage arrays e-Series

Em uma configuração Stretch MetroCluster com um storage array LUNs e-Series, você pode conetar diretamente os controladores de armazenamento e os arrays de armazenamento. Ao contrário de outros LUNs de array, os switches FC não são necessários.

O "Suporte de conexão direta para configuração Stretch MetroCluster com array NetApp e-Series"artigo da base de conhecimento fornece exemplos de configurações com LUNs de array e-Series.

Considerações ao remover configurações do MetroCluster

Você pode remover a configuração do MetroCluster de todos os nós em um grupo de recuperação de desastres (DR). Depois de remover a configuração do MetroCluster, toda a conetividade de disco e interconexões devem ser ajustadas para estar em um estado suportado. Se precisar remover a configuração do MetroCluster, entre em Contato com o suporte técnico.

Não é possível reverter a desconfiguração do MetroCluster. Este processo só deve ser feito com a assistência de suporte técnico. Entre em Contato com o suporte técnico da NetApp e consulte o guia apropriado para sua configuração no "Como remover nós de uma configuração MetroCluster - Guia de resolução."

Como usar o Active IQ Unified Manager e o Gerenciador de sistemas ONTAP para configuração e monitoramento adicionais

Uso do Active IQ Unified Manager e do Gerenciador de sistemas do ONTAP para configuração e monitoramento adicionais

O Active IQ Unified Manager e o ONTAP System Manager podem ser usados para o gerenciamento de GUI dos clusters e para o monitoramento da configuração.

Cada nó tem o Gerenciador de sistema do ONTAP pré-instalado. Para carregar o System Manager, insira o endereço LIF de gerenciamento de cluster como URL em um navegador da Web que tem conetividade com o nó.

Você também pode usar o Active IQ Unified Manager para monitorar a configuração do MetroCluster.

Informações relacionadas

"Documentação do Gestor de sistemas Active IQ Unified Manager e ONTAP"

Sincronizar a hora do sistema usando NTP

Cada cluster precisa de seu próprio servidor NTP (Network Time Protocol) para sincronizar o tempo entre os nós e seus clientes. Você pode usar a caixa de diálogo Editar DateTime no System Manager para configurar o servidor NTP.

Verifique se você baixou e instalou o System Manager. O Gerenciador do sistema está disponível no site de suporte da NetApp.

- Não é possível modificar as configurações de fuso horário para um nó com falha ou para o nó do parceiro após a aquisição ocorrer.
- Cada cluster na configuração do MetroCluster FC deve ter seu próprio servidor NTP separado ou servidores usados pelos nós e (se houver) pontes FC para SAS nesse local do MetroCluster.

  Se você estiver usando o software tiebreaker do MetroCluster, ele também deve ter seu próprio servidor NTP separado.

Passos

1. Na página inicial, clique duas vezes no sistema de armazenamento apropriado.
2. Expanda a hierarquia **Cluster** no painel de navegação esquerdo.
3. No painel de navegação, clique em **Configuração** > **Ferramentas do sistema** > **DateTime**.
4. Clique em **Editar**.
5. Selecione o fuso horário.
6. Especifique os endereços IP dos servidores de hora e clique em **Adicionar**.

   Você deve adicionar um servidor NTP à lista de servidores de hora. O controlador de domínio pode ser um servidor autorizado.

7. Clique em **OK**.
8. Verifique as alterações feitas nas configurações de data e hora na janela Data e hora.

Considerações ao usar o ONTAP em uma configuração do MetroCluster

Ao usar o ONTAP em uma configuração do MetroCluster, você deve estar ciente de certas considerações sobre licenciamento, peering para clusters fora da configuração do MetroCluster, execução de operações de volume, operações NVFAIL e outras operações do ONTAP.

Considerações sobre licenciamento

- Ambos os sites devem ser licenciados para os mesmos recursos licenciados pelo site.
- Todos os nós devem ser licenciados para os mesmos recursos de bloqueio de nó.

Consideração de SnapMirror

- A recuperação de desastres do SnapMirror SVM só é compatível com configurações do MetroCluster

executando versões do ONTAP 9.5 ou posterior.

Suporte FlexCache em uma configuração MetroCluster

A partir do ONTAP 9.7, os volumes FlexCache são compatíveis com configurações do MetroCluster. Você deve estar ciente dos requisitos para a repetibilidade manual após operações de comutação ou switchback.

Repetibilidade da SVM após o switchover quando a origem e o cache do FlexCache estão no mesmo local do MetroCluster

Após um switchover negociado ou não planejado, qualquer relacionamento de peering SVM FlexCache no cluster deve ser configurado manualmente.

Por exemplo, svms VS1 (cache) e VS2 (origem) estão no site_A. Esses SVMs são peered.

Após o switchover, os svms VS1-MC e VS2-mc são ativados no local do parceiro (site_B). Eles devem ser manualmente repelidos para que o FlexCache funcione usando o `vserver peer repeer` comando.

Repetibilidade da SVM após switchover ou switchback quando um destino FlexCache está em um terceiro cluster e no modo desconetado

Para as relações do FlexCache com um cluster fora da configuração do MetroCluster, o peering deve ser sempre reconfigurado manualmente após um switchover quando os clusters envolvidos estão em um modo desconetado durante o switchover.

Por exemplo:

- Um fim do FlexCache (cache_1 no VS1) reside no MetroCluster site_A tem um fim do FlexCache
- A outra extremidade do FlexCache (origin_1 no VS2) reside no site_C (não na configuração do MetroCluster)

Quando o switchover é acionado e se o site_A e o site_C não estiverem conetados, você deverá repelir manualmente os SVMs no site_B (o cluster de switchover) e site_C usando o `vserver peer repeer` comando após o switchover.

Quando o switchback é executado, você deve repelir novamente os SVMs no site_A (o cluster original) e site_C.

Suporte FabricPool em configurações MetroCluster

A partir do ONTAP 9.7, as configurações do MetroCluster são compatíveis com camadas de storage FabricPool.

Para obter informações gerais sobre como usar o FabricPools, consulte "Gerenciamento de discos e agregados".

Considerações ao usar FabricPools

- Os clusters precisam ter licenças FabricPool com limites de capacidade correspondentes.
- Os clusters devem ter IPspaces com nomes correspondentes.

  Esse pode ser o espaço IPspace padrão ou um espaço IP criado por um administrador. Este espaço IPspace será usado para configurações de armazenamento de objetos FabricPool.

- Para o espaço IPspace selecionado, cada cluster deve ter um LIF entre clusters definido que possa alcançar o armazenamento de objetos externo

Configurando um agregado para uso em um FabricPool espelhado

Antes de configurar o agregado, você deve configurar armazenamentos de objetos conforme descrito em "Configurando armazenamentos de objetos para FabricPool em uma configuração MetroCluster" no "Gerenciamento de discos e agregados".

Para configurar um agregado para uso em um FabricPool:

1. Crie o agregado ou selecione um agregado existente.
2. Espelhe o agregado como um agregado espelhado típico na configuração do MetroCluster.
3. Crie o espelho FabricPool com o agregado, conforme descrito no "Gerenciamento de discos e agregados":
   a. Anexe um armazenamento de objetos primário.

      Este armazenamento de objetos está fisicamente mais perto do cluster.

   b. Adicione um armazenamento de objetos espelhados.

      Este armazenamento de objetos está fisicamente mais longe do cluster do que o armazenamento de objetos principal.

Suporte FlexGroup em configurações MetroCluster

A partir do ONTAP 9.6, as configurações do MetroCluster são compatíveis com volumes FlexGroup.

Programações de trabalhos em uma configuração MetroCluster

No ONTAP 9.3 e posterior, as programações de tarefas criadas pelo usuário são replicadas automaticamente entre clusters em uma configuração do MetroCluster. Se você criar, modificar ou excluir um agendamento de trabalho em um cluster, o mesmo agendamento será criado automaticamente no cluster de parceiros, usando o CRS (Configuration Replication Service).

As programações criadas pelo sistema não são replicadas e você deve executar manualmente a mesma operação no cluster de parceiros para que as programações de tarefas em ambos os clusters sejam idênticas.

Peering de cluster do site MetroCluster para um terceiro cluster

Como a configuração de peering não é replicada, se você identificar um dos clusters na configuração do MetroCluster para um terceiro cluster fora dessa configuração, você também deverá configurar o peering no cluster do MetroCluster parceiro. Isso é para que o peering possa ser mantido se ocorrer um switchover.

O cluster que não é MetroCluster deve estar executando o ONTAP 8,3 ou posterior. Caso contrário, o peering é perdido se ocorrer um switchover, mesmo que o peering tenha sido configurado em ambos os parceiros da MetroCluster.

Replicação de configuração de cliente LDAP em uma configuração MetroCluster

Uma configuração de cliente LDAP criada em uma máquina virtual de storage (SVM) em um cluster local é replicada para os dados de parceiros SVM no cluster remoto. Por exemplo, se a configuração do cliente LDAP for criada no SVM admin no cluster local, ela será replicada para todos os SVMs de dados administrativos no cluster remoto. Esse recurso do MetroCluster é intencional para que a configuração do cliente LDAP esteja ativa em todos os SVMs de parceiros no cluster remoto.

Diretrizes de criação de LIF e rede para configurações do MetroCluster

Você deve estar ciente de como LIFs são criados e replicados em uma configuração do MetroCluster. Você também deve saber sobre o requisito de consistência para que você possa tomar as decisões adequadas ao configurar sua rede.

Informações relacionadas

"Conceitos de ONTAP"

Requisitos de replicação de objeto IPspace e configuração de sub-rede

Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

Replicação IPspace

Você deve considerar as diretrizes a seguir enquanto replica objetos IPspace para o cluster de parceiros:

- Os nomes de IPspace dos dois locais devem corresponder.
- Os objetos IPspace devem ser replicados manualmente para o cluster do parceiro.

  Quaisquer máquinas virtuais de armazenamento (SVMs) que sejam criadas e atribuídas a um IPspace antes que o IPspace seja replicado não serão replicadas para o cluster de parceiros.

Configuração de sub-rede

Você deve considerar as seguintes diretrizes ao configurar sub-redes em uma configuração do MetroCluster:

- Ambos os clusters da configuração do MetroCluster devem ter uma sub-rede no mesmo espaço IPspace com o mesmo nome de sub-rede, sub-rede, domínio de broadcast e gateway.
- Os intervalos de IP dos dois clusters devem ser diferentes.

  No exemplo a seguir, os intervalos de IP são diferentes:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------       -------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      --------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.21-192.168.2.30
```

Configuração IPv6

Se o IPv6 estiver configurado em um site, o IPv6 também deve ser configurado no outro site.

Requisitos para criação de LIF em uma configuração MetroCluster

Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

Você deve considerar as seguintes diretrizes ao criar LIFs:

- Fibre Channel: Você precisa usar VSAN esticada ou tecidos esticados.
- IP/iSCSI: Você deve usar a rede estendida da camada 2.
- Broadcasts ARP: Você deve habilitar broadcasts ARP entre os dois clusters.
- LIFs duplicadas: Você não deve criar vários LIFs com o mesmo endereço IP (LIFs duplicadas) em um espaço IPspace.
- Configurações NFS e SAN: Você precisa usar diferentes máquinas virtuais de storage (SVMs) para agregados sem espelhamento e espelhados.
- Você deve criar um objeto de sub-rede antes de criar um LIF. Um objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque tem um domínio de broadcast associado.

Verifique a criação de LIF

Você pode confirmar a criação bem-sucedida de um LIF em uma configuração do MetroCluster executando o `metrocluster check lif show` comando. Se você encontrar algum problema ao criar o LIF, você pode usar o `metrocluster check lif repair-placement` comando para corrigir os problemas.

Requisitos e problemas de replicação e posicionamento de LIF

Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

Replicação de LIFs para o cluster de parceiros

Quando você cria um LIF em um cluster em uma configuração do MetroCluster, o LIF é replicado no cluster de parceiros. LIFs não são colocados em uma base de nome individual. Para disponibilidade de LIFs após uma operação de switchover, o processo de colocação de LIF verifica se as portas são capazes de hospedar o LIF com base em verificações de acessibilidade e atributos de porta.

O sistema deve atender às seguintes condições para colocar as LIFs replicadas no cluster de parceiros:

Condição	Tipo de LIF: FC	Tipo de LIF: IP/iSCSI
Identificação do nó	O ONTAP tenta colocar o LIF replicado no parceiro de recuperação de desastres (DR) do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.	O ONTAP tenta colocar o LIF replicado no parceiro de DR do nó no qual ele foi criado. Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.
Identificação da porta	O ONTAP identifica as portas de destino FC conectadas no cluster de DR.	As portas no cluster de DR que estão no mesmo espaço IPspace que o LIF de origem são selecionadas para uma verificação de acessibilidade. Se não houver portas no cluster de DR no mesmo IPspace, o LIF não pode ser colocado. Todas as portas no cluster de DR que já estão hospedando um LIF no mesmo espaço IPspace e sub-rede são marcadas automaticamente como alcançáveis e podem ser usadas para o posicionamento. Essas portas não estão incluídas na verificação de acessibilidade.

Verificação de acessibilidade	A acessibilidade é determinada verificando a conetividade da malha de origem WWN nas portas do cluster de DR. Se a mesma malha não estiver presente no local de DR, o LIF será colocado em uma porta aleatória no parceiro de DR.	A acessibilidade é determinada pela resposta a um broadcast ARP (Address Resolution Protocol) de cada porta identificada anteriormente no cluster de DR para o endereço IP de origem do LIF a ser colocado. Para que as verificações de acessibilidade sejam bem-sucedidas, os broadcasts ARP devem ser permitidos entre os dois clusters. Cada porta que recebe uma resposta do LIF de origem será marcada como possível para o posicionamento.
Seleção da porta	O ONTAP categoriza as portas com base em atributos como tipo e velocidade do adaptador e, em seguida, seleciona as portas com atributos correspondentes. Se nenhuma porta com atributos correspondentes for encontrada, o LIF será colocado em uma porta conetada aleatória no parceiro DR.	A partir das portas marcadas como alcançáveis durante a verificação de acessibilidade, o ONTAP prefere as portas que estão no domínio de broadcast associado à sub-rede do LIF. Se não houver portas de rede disponíveis no cluster de DR que estejam no domínio de broadcast associado à sub-rede do LIF, o ONTAP selecionará portas que tenham acessibilidade ao LIF de origem. Se não houver portas com acessibilidade ao LIF de origem, uma porta será selecionada do domínio de broadcast associado à sub-rede do LIF de origem e, se nenhum domínio de broadcast existir, uma porta aleatória será selecionada. O ONTAP categoriza as portas com base em atributos como tipo de adaptador, tipo de interface e velocidade e, em seguida, seleciona as portas com atributos correspondentes.

Colocação de LIF	A partir das portas alcançáveis, o ONTAP seleciona a porta menos carregada para colocação.	A partir das portas selecionadas, o ONTAP seleciona a porta menos carregada para colocação.

Colocação de LIFs replicadas quando o nó do parceiro de DR está inativo

Quando um iSCSI ou FC LIF é criado em um nó cujo parceiro de DR foi assumido, o LIF replicado é colocado no nó do parceiro auxiliar de DR. Após uma operação subsequente de giveback, os LIFs não são movidos automaticamente para o parceiro DR. Isso pode levar a que os LIFs se concentrem em um único nó no cluster de parceiros. Durante uma operação de switchover do MetroCluster, tentativas subsequentes de mapear LUNs pertencentes à máquina virtual de storage (SVM) falham.

Você deve executar o `metrocluster check lif show` comando após uma operação de aquisição ou operação de giveback para verificar se o posicionamento de LIF está correto. Se existirem erros, pode executar o `metrocluster check lif repair-placement` comando para resolver os problemas.

Erros de colocação de LIF

Os erros de colocação de LIF que são exibidos pelo `metrocluster check lif show` comando são retidos após uma operação de comutação. Se o `network interface modify` comando , `network interface rename` ou `network interface delete` for emitido para um LIF com um erro de posicionamento, o erro será removido e não aparecerá na saída do `metrocluster check lif show` comando.

Falha de replicação de LIF

Você também pode verificar se a replicação do LIF foi bem-sucedida usando o `metrocluster check lif show` comando. Uma mensagem EMS é exibida se a replicação LIF falhar.

Você pode corrigir uma falha de replicação executando o `metrocluster check lif repair-placement` comando para qualquer LIF que não consiga encontrar uma porta correta. Você deve resolver quaisquer falhas de replicação de LIF o mais rápido possível para verificar a disponibilidade de LIF durante uma operação de switchover de MetroCluster.

> Mesmo que o SVM de origem esteja inativo, o posicionamento de LIF pode continuar normalmente se houver um LIF pertencente a um SVM diferente em uma porta com o mesmo espaço IPspace e rede no SVM de destino.

Criação de volume em um agregado raiz

O sistema não permite a criação de novos volumes no agregado raiz (um agregado com uma política de HA do CFO) de um nó em uma configuração do MetroCluster.

Devido a essa restrição, os agregados de raiz não podem ser adicionados a um SVM usando o `vserver add-aggregates` comando.

Recuperação de desastres do SVM em uma configuração de MetroCluster

A partir do ONTAP 9.5, as máquinas virtuais de storage ativo (SVMs) em uma configuração do MetroCluster podem ser usadas como fontes com o recurso de recuperação de desastres do SnapMirror SVM. O SVM de destino deve estar no terceiro cluster fora da configuração do MetroCluster.

Você deve estar ciente dos seguintes requisitos e limitações de uso de SVMs com recuperação de desastres

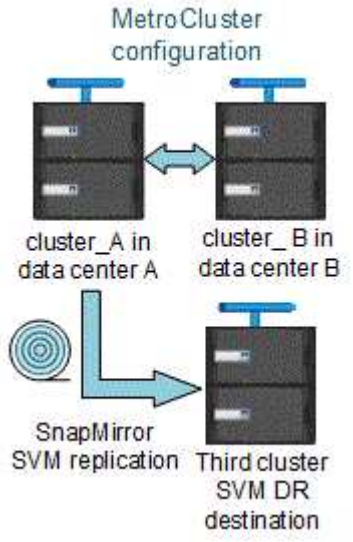
do SnapMirror:

- Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM.

  Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover.

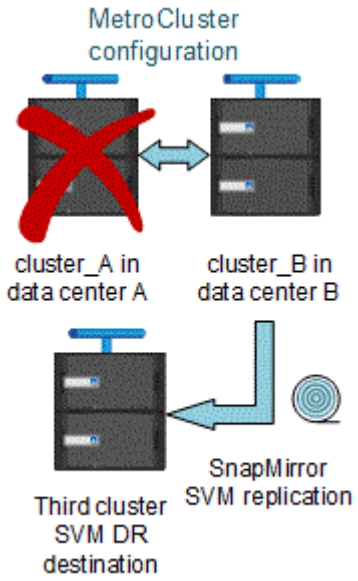
- Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online.

  A imagem a seguir mostra o comportamento de recuperação de desastres do SVM em um estado estável:



- Quando o SVM de origem sincronizada é a fonte de uma relação SVM DR, as informações de origem no relacionamento de SVM DR são replicadas para o parceiro MetroCluster.

  Isso permite que as atualizações do SVM DR continuem após um switchover, conforme mostrado na imagem a seguir:



- Durante os processos de switchover e switchback, a replicação para o destino SVM DR pode falhar.

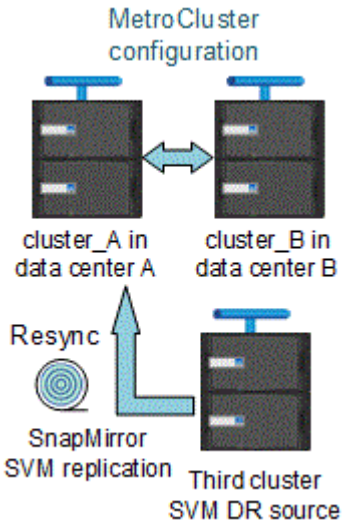
  No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas do SVM DR serão bem-sucedidas.

Consulte a seção ""replicando a configuração do SVM"" no "Proteção de dados com a CLI" para obter detalhes sobre como configurar um relacionamento de DR do SVM.

Ressincronização da SVM em um local de recuperação de desastre

Durante a ressincronização, a fonte de recuperação de desastres (DR) de máquinas virtuais de storage (SVMs) na configuração MetroCluster é restaurada a partir do SVM de destino no local que não é MetroCluster.

Durante a ressincronização, o SVM de origem (cluster_A) atua temporariamente como SVM de destino, conforme mostrado na imagem a seguir:



Se um switchover não planejado ocorrer durante a ressincronização

Switchovers não planejados que ocorrem durante a ressincronização interromperão a transferência de ressincronização. Se ocorrer um switchover não planejado, as seguintes condições são verdadeiras:

- O SVM de destino no local do MetroCluster (que era uma fonte SVM antes da ressincronização) permanece como um SVM de destino. O SVM no cluster de parceiros continuará mantendo seu subtipo e inativo.
- A relação do SnapMirror deve ser recriada manualmente com o SVM de destino de sincronização como destino.
- A relação SnapMirror não aparece na saída do show do SnapMirror após um switchover no local sobrevivente, a menos que uma operação de criação do SnapMirror seja executada.

Execução do switchback após um switchover não planejado durante a ressincronização

Para executar com sucesso o processo de switchback, a relação de ressincronização deve ser quebrada e excluída. O switchback não é permitido se houver algum SVMs de destino de DR do SnapMirror na configuração do MetroCluster ou se o cluster tiver um SVM de subtipo "dp-destination".

Saída dos comandos show de disco de armazenamento e shelf de armazenamento show show em uma configuração Stretch MetroCluster de dois nós

Em uma configuração Stretch MetroCluster de dois nós, `is-local-attach` o campo dos `storage disk show` comandos e `storage shelf show` mostra todos os discos e compartimentos de storage como locais, independentemente do nó ao qual eles estão conetados.

A saída para o comando storage Aggregate plex show é indeterminada após um switchover do MetroCluster

Quando você executa o `storage aggregate plex show` comando após um switchover do MetroCluster, o status de plex0 do agregado de raiz comutada é indeterminado e é exibido como `failed`. Durante este tempo, a raiz comutada não é atualizada. O estado real deste Plex só pode ser determinado após a fase de cicatrização do MetroCluster.

Modificação de volumes para definir o sinalizador NVFAIL em caso de comutação

Você pode modificar um volume para que o sinalizador NVFAIL seja definido no volume em caso de um switchover MetroCluster. O sinalizador NVFAIL faz com que o volume seja vedado de qualquer modificação. Isso é necessário para volumes que precisam ser tratados como se as gravações confirmadas no volume fossem perdidas após o switchover.

Nas versões do ONTAP anteriores a 9,0, o sinalizador NVFAIL é usado para cada switchover. No ONTAP 9.0 e versões posteriores, o switchover não planejado (USO) é usado.

Passos

1. Ative a configuração do MetroCluster para acionar o NVFAIL no switchover definindo o `vol -dr-force -nvfail` parâmetro como "'on'":

   `vol modify -vserver` *`vserver-name`* `-volume` *`volume-name`* `-dr-force-nvfail on`

Transição de uma configuração MetroCluster elástica para uma configuração de malha

Em uma configuração MetroCluster conectada à malha, os nós estão em diferentes locais. Essa diferença geográfica aumenta a proteção contra desastres. Para fazer a transição de uma configuração Stretch para uma MetroCluster conectada à malha, é necessário adicionar switches FC e, se necessário, pontes FC para SAS à configuração.

- Você deve desativar o switchover automático em ambos os clusters executando o `metrocluster modify -auto-switchover-failure-domain auto-disabled` comando.
- Você precisa ter encerrado os nós.

  Este procedimento é disruptivo.

A configuração do MetroCluster deve ser transferida em ambos os sites. Após atualizar a configuração do MetroCluster, você precisa habilitar o switchover automático nos dois clusters. Também é necessário validar a configuração executando o `metrocluster check run` comando.

Este procedimento fornece uma visão geral dos passos necessários. Para obter instruções detalhadas, consulte as seções específicas do "Instalação e configuração do MetroCluster conectado à malha". Você não precisa fazer uma instalação e configuração completas.

Passos

1. Prepare-se para a atualização revisando cuidadosamente a seção "preparação para a instalação do MetroCluster" do "Instalação e configuração do MetroCluster conectado à malha".
2. Instale, faça cabos e configure os switches e as bridges FC-para-SAS necessários.

   Você deve usar os procedimentos na seção "cabeamento de uma configuração de MetroCluster conetada à malha" do "Instalação e configuração do MetroCluster conectado à malha".

3. Atualize a configuração do MetroCluster usando as etapas a seguir.

   Não use os procedimentos na seção "Configurando o software MetroCluster no ONTAP" localizada no "Instalação e configuração do MetroCluster conectado à malha".

   a. Entre no modo de privilégio avançado
   `set -privilege advanced`

   b. Atualize a configuração do MetroCluster
   `metrocluster configure -refresh true`

   O comando a seguir atualiza a configuração do MetroCluster em todos os nós do grupo DR que contém controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

   a. Voltar ao modo de privilégio de administrador
   `set -privilege admin`

4. Verifique se há erros na configuração do MetroCluster e verifique se ela está operacional.

   Você deve usar os procedimentos nas seções a seguir do "Instalação e configuração do MetroCluster conectado à malha":

   - Verificando erros de configuração do MetroCluster com o Config Advisor
   - Verificação da operação local de HA
   - Verificando switchover, cura e switchback

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto

"Documentação do ONTAP 9"	• Todos os guias MetroCluster
	• Uma visão geral técnica da configuração e operação do MetroCluster FC. • Práticas recomendadas para configuração MetroCluster FC.
"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do IP MetroCluster: Diferenças entre as configurações do ONTAP MetroCluster"	• Arquitetura IP do MetroCluster • Fazer o cabeamento da configuração • Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster e recuperação de desastres"	• Compreender a configuração do MetroCluster • Switchover, cura e switchback • Recuperação de desastres (DR)
"Mantenha os componentes do MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster FC • Substituição ou atualização de hardware. Procedimentos de atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conetada à malha • Substituição do hardware em um local de recuperação de desastres em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.

"Transição do MetroCluster FC para o MetroCluster IP" "Guia de atualização e expansão do MetroCluster"	• Atualizando ou atualizando uma configuração do MetroCluster • Transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP • Expansão de uma configuração do MetroCluster com a adição de nós adicionais
"Instalação e configuração do software MetroCluster Tiebreaker"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
Documentação do Active IQ Unified Manager "Documentação do NetApp: Guias de produto e recursos"	• Monitoramento da configuração e do desempenho do MetroCluster
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
"Conceitos de ONTAP"	• Como os agregados espelhados funcionam

Instale e configure o tiebreaker do MetroCluster

O que há de novo

As melhorias no software tiebreaker MetroCluster são fornecidas em cada versão. Veja o que há de novo em lançamentos recentes do MetroCluster Tiebreaker.

Melhorias

Versão de desempate do ONTAP	Melhorias
1.6P1	• Atualização de bibliotecas de suporte • Melhorias de segurança
1,6	• Maior facilidade de instalação • Atualização de bibliotecas de suporte • Melhorias de segurança
1,5	• Atualização de bibliotecas de suporte • Melhorias de segurança
1,4	• Atualização de bibliotecas de suporte

Matriz de suporte de SO

A tabela a seguir indica os sistemas operacionais suportados para cada versão do tiebreaker.

SO para desempate	1.6P1	1,6	1,5	1,4
Rocky Linux 9,4	Sim	Não	Não	Não
Rocky Linux 9,0	Não	Sim	Não	Não
Rocky Linux 8,10	Sim	Não	Não	Não
Chapéu vermelho 9,4	Sim	Não	Não	Não
Chapéu vermelho 9,3	Não	Não	Não	Não
Chapéu vermelho 9,2	Sim	Sim	Não	Não

Chapéu vermelho 9,1	Não	Sim	Não	Não
Chapéu vermelho 9,0	Não	Sim	Não	Não
Red Hat 8,11 - 9,0	Não	Sim	Não	Não
Chapéu vermelho 8,10	Sim	Sim	Não	Não
Chapéu vermelho 8,9	Não	Sim	Não	Não
Chapéu vermelho 8,8	Sim	Sim	Não	Não
Red Hat 8,1 - 8,7	Não	Sim	Sim	Sim
Red Hat 7 - 7,9	Não	Não	Não	Sim
CentOS 7 - 7,9	Não	Não	Não	Sim

Visão geral do software tiebreaker

É útil entender o que é o software tiebreaker da NetApp MetroCluster e como ele distingue entre os tipos de falhas para que você possa monitorar suas configurações do MetroCluster com eficiência. Use a CLI do tiebreaker para gerenciar configurações e monitorar o status e as operações das configurações do MetroCluster.

Detecção de falhas com o software tiebreaker NetApp MetroCluster

Você só precisa do software tiebreaker se quiser monitorar dois clusters e o status de conectividade entre eles em um terceiro local. O software tiebreaker reside em um host Linux no terceiro local e permite que cada parceiro em um cluster faça a distinção entre uma falha ISL, quando os links entre sites estão inativos, de uma falha do local.

Depois de instalar o software tiebreaker em um host Linux, é possível configurar os clusters em uma configuração do MetroCluster para monitorar as condições de desastre.

O software tiebreaker pode monitorar até 15 configurações de MetroCluster simultaneamente. Ele dá suporte a uma combinação de configurações MetroCluster IP, MetroCluster FC e Stretch MetroCluster.

Como o software tiebreaker deteta falhas no local

O software tiebreaker do NetApp MetroCluster verifica a acessibilidade dos nós em uma configuração do MetroCluster e do cluster para determinar se ocorreu uma falha no local. O software tiebreaker também aciona um alerta sob certas condições.

Componentes monitorados pelo software tiebreaker

O software tiebreaker monitora cada controladora na configuração do MetroCluster estabelecendo conexões redundantes por meio de vários caminhos para um LIF de gerenciamento de nós e para o LIF de gerenciamento de cluster, ambos hospedados na rede IP.

O software tiebreaker monitora os seguintes componentes na configuração do MetroCluster:

- Nós por meio de interfaces de nós locais
- Cluster por meio das interfaces designadas por cluster
- Cluster sobrevivente para avaliar se ele tem conetividade com o local de desastre (interconexão NV, armazenamento e peering entre clusters)

Quando houver uma perda de conexão entre o software tiebreaker e todos os nós no cluster e para o próprio cluster, o cluster será declarado como "não alcançável" pelo software tiebreaker. Demora cerca de três a cinco segundos para detetar uma falha de ligação. Se um cluster não estiver acessível a partir do software tiebreaker, o cluster sobrevivente (o cluster que ainda está acessível) deve indicar que todos os links para o cluster de parceiros são cortados antes que o software tiebreaker acione um alerta.

Todos os links são cortados se o cluster sobrevivente não puder mais se comunicar com o cluster no local de desastre por meio de FC (interconexão e armazenamento NV) e peering entre clusters.

Cenários de falha durante os quais o software tiebreaker aciona um alerta

O software tiebreaker aciona um alerta quando o cluster (todos os nós) no local de desastre está inativo ou inacessível e o cluster no local sobrevivente indica o status "'AllLinksSevered'".

O software tiebreaker não aciona um alerta (ou o alerta é vetado) nos seguintes cenários:

- Em uma configuração de MetroCluster de oito nós, se um par de HA no local de desastre estiver inativo
- Em um cluster com todos os nós no local do desastre para baixo, um par de HA no local sobrevivente para baixo, e o cluster no local sobrevivente indica o status ""AllLinksSevered""

  O software tiebreaker aciona um alerta, mas o ONTAP veta esse alerta. Nesta situação, também é vetado um switchover manual

- Qualquer cenário em que o software tiebreaker possa alcançar pelo menos um nó ou a interface de cluster no local de desastre, ou o local sobrevivente ainda pode alcançar qualquer nó no local de desastre por meio de FC (interconexão e storage NV) ou peering entre clusters

Informações relacionadas

"Riscos e limitações do uso do MetroCluster Tiebreaker no modo ativo"

Como o software tiebreaker deteta falhas de conetividade entre sites

O software tiebreaker do MetroCluster alerta você se toda a conetividade entre os sites for perdida.

Tipos de caminhos de rede

Dependendo da configuração, existem três tipos de caminhos de rede entre os dois clusters em uma configuração MetroCluster:

- **Rede FC (presente em configurações MetroCluster conetadas à malha)**

  Esse tipo de rede é composto por duas malhas de switch FC redundantes. Cada malha de switch tem dois switches FC, com um switch de cada malha de switch colocado com um cluster. Cada cluster tem dois switches FC, um de cada malha de switch. Todos os nós têm conectividade FC (interconexão NV e iniciador FCP) a cada um dos switches FC colocalizados. Os dados são replicados de cluster para cluster através do ISL.

- **Rede de peering entre clusters**

  Este tipo de rede é composto por um caminho de rede IP redundante entre os dois clusters. A rede de peering de cluster fornece a conectividade necessária para espelhar a configuração da máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada pelo cluster de parceiros.

- **Rede IP (presente nas configurações IP do MetroCluster)**

  Este tipo de rede é composto por duas redes de switch IP redundantes. Cada rede tem dois switches IP, com um switch de cada malha de switch co-localizado com um cluster. Cada cluster tem dois switches IP, um de cada malha de switch. Todos os nós têm conectividade a cada um dos switches FC colocalizados. Os dados são replicados de cluster para cluster através do ISL.

Monitoramento da conetividade entre sites

O software tiebreaker recupera regularmente o status da conetividade entre sites dos nós. Se a conetividade de interconexão NV for perdida e o peering entre clusters não responder a pings, os clusters assumem que os sites estão isolados e o software tiebreaker aciona um alerta como ""AllLinksSevered"". Se um cluster identificar o status ""AllLinksSevered"" e o outro cluster não estiver acessível através da rede, o software tiebreaker aciona um alerta como "disaster".

Como diferentes tipos de desastre afetam o tempo de deteção do software tiebreaker

Para um melhor Planejamento de recuperação de desastres, o software tiebreaker da MetroCluster leva algum tempo para detetar um desastre. Este tempo gasto é o "tempo de deteção do "usuário". O software tiebreaker do MetroCluster deteta o desastre no local em 30 segundos a partir do momento da ocorrência do desastre e aciona a operação de recuperação de desastres para notificá-lo sobre o desastre.

O tempo de deteção também depende do tipo de desastre e pode exceder 30 segundos em alguns cenários, principalmente conhecidos como ""desastres rolantes"". Os principais tipos de desastre contínuo são os seguintes:

- Perda de energia
- Pânico
- Parar ou reiniciar
- Perda de switches FC no local de desastre

Perda de energia

O software tiebreaker aciona imediatamente um alerta quando o nó deixa de funcionar. Quando há uma perda de energia, todas as conexões e atualizações, como peering entre clusters, interconexão NV e disco de caixa de correio, param. O tempo decorrido entre o cluster se tornar inacessível, a deteção do desastre e o gatilho, incluindo o tempo de silêncio padrão de 5 segundos, não deve exceder 30 segundos.

Pânico

Nas configurações do MetroCluster FC, o software tiebreaker aciona um alerta quando a conexão de interconexão NV entre os sites está inativa e o site sobrevivente indica o status ""AllLinksSevered"". Isso só acontece depois que o processo de coredump estiver concluído. Nesse cenário, o tempo decorrido entre o cluster e a deteção de um desastre pode ser maior ou aproximadamente igual ao tempo necessário para o processo de coredump. Em muitos casos, o tempo de deteção é superior a 30 segundos.

Se um nó parar de funcionar, mas não gerar um arquivo para o processo de coredump, o tempo de deteção não deve ser superior a 30 segundos. Nas configurações IP do MetroCluster, o NV pára de se comunicar e o site sobrevivente não está ciente do processo de coredump.

Parar ou reiniciar

O software tiebreaker aciona um alerta apenas quando o nó está inativo e o site sobrevivente indica o status "'AllLinksSevered". O tempo necessário entre o cluster se tornar inacessível e a deteção de um desastre pode ser superior a 30 segundos. Nesse cenário, o tempo necessário para detectar um desastre depende de quanto tempo leva para que os nós no local do desastre sejam desligados.

Perda de switches FC no local de desastre (configuração de MetroCluster conectada à malha)

O software tiebreaker aciona um alerta quando um nó deixa de funcionar. Se os switches FC forem perdidos, o nó tentará recuperar o caminho para um disco por cerca de 30 segundos. Durante esse tempo, o nó está ativo e respondendo na rede de peering. Quando ambos os switches FC estão inativos e o caminho para um disco não pode ser recuperado, o nó produz um erro MultiDiskFailure e pára. O tempo decorrido entre a falha do switch FC e o número de vezes que os nós produziram erros MultiDiskFailure é cerca de 30 segundos mais longo. Esses 30 segundos adicionais devem ser adicionados ao tempo de deteção de desastres.

Sobre a CLI e as páginas man do tiebreaker

A CLI do tiebreaker fornece comandos que permitem configurar remotamente o software tiebreaker e monitorar as configurações do MetroCluster.

O prompt de comando da CLI é representado como NetApp MetroCluster tiebreaker::>.

As páginas man estão disponíveis na CLI inserindo o nome do comando aplicável no prompt.

Instale o software tiebreaker

Fluxo de trabalho de instalação do tiebreaker

O software tiebreaker fornece recursos de monitoramento para um ambiente de storage em cluster. Ele também envia notificações SNMP em caso de problemas de conetividade de nó e desastres de site.

Sobre este fluxo de trabalho

Você pode usar esse fluxo de trabalho para instalar ou atualizar o software tiebreaker.

1. **"Prepare-se para instalar o software tiebreaker"**

Antes de instalar e configurar o software tiebreaker, verifique se o sistema atende a certos requisitos.

2 **"Fixe a instalação"**

Para configurações que executam o MetroCluster tiebreaker 1,5 e posterior, você pode proteger e proteger o sistema operacional do host e o banco de dados.

3 **"Instale o pacote de software tiebreaker"**

Execute uma nova instalação ou atualização do software tiebreaker. O procedimento de instalação a seguir depende da versão do tiebreaker que você deseja instalar.

Prepare-se para instalar o software tiebreaker

Antes de instalar e configurar o software tiebreaker, você deve verificar se o sistema atende a certos requisitos.

Requisitos de software

Você precisa atender aos seguintes requisitos de software, dependendo da versão do tiebreaker que você está instalando.

Versão de desempate do ONTAP	Versões de ONTAP compatíveis	Versões Linux suportadas	Requisitos Java/MariaDB
1.6P1	ONTAP 9.12,1 e posterior	Consulte "Matriz de suporte DO SO"para obter mais informações.	Nenhum. As dependências são empacotadas com a instalação.
1,6	ONTAP 9.12,1 e posterior	Consulte "Matriz de suporte DO SO"para obter mais informações.	Nenhum. As dependências são empacotadas com a instalação.
1,5	ONTAP 9 F.8 a ONTAP 9.14,1	• Red Hat Enterprise Linux 8,1 a 8,7	Com o Red Hat Enterprise Linux 8,1 a 8,7: • MariaDB 10.x (use a versão padrão que é instalada usando "yum install mariadb-server.x86_64") • OpenJDK 17, 18 ou 19

1,4	ONTAP 9 F.1 para ONTAP 9.9,1	• Red Hat Enterprise Linux 8,1 a 8,7 • Red Hat Enterprise Linux 7 a 7,9 • CentOS 7 a 7,9 64 bits	Com CentOS: • MariaDB 5,5.52.x/MySQL Server 5,6x • 4 GB DE RAM • Abra o JRE 8 Com o Red Hat Enterprise Linux 8,1 a 8,7: • MariaDB 10.x (use a versão padrão que é instalada usando "yum install mariadb-server.x86_64") • JRE 8

Requisitos adicionais

Você deve estar ciente dos seguintes requisitos adicionais:

- O software tiebreaker é instalado em um terceiro local, o que permite que o software faça a distinção entre uma falha de enlace inter-switch (ISL) (quando os links entre locais estão inoperantes) e uma falha no local. O sistema de host precisa atender a certos requisitos antes de instalar ou atualizar o software tiebreaker para monitorar a configuração do MetroCluster.
- Você deve ter o Privileges "root" para instalar o software tiebreaker do MetroCluster e os pacotes dependentes.
- Você só pode usar um monitor de desempate do MetroCluster por configuração do MetroCluster para evitar qualquer conflito com vários monitores de desempate.
- Ao selecionar a fonte NTP (Network Time Protocol) para o software tiebreaker, você deve usar uma fonte NTP local. O software tiebreaker não deve usar a mesma fonte que os sites do MetroCluster que o software tiebreaker monitora.
- Capacidade do disco: 8 GB
- Firewall:
  - Acesso direto para configurar mensagens AutoSupport
  - SSH (porta 22/TCP), HTTPS (porta 443/TCP) e ping (ICMP)

Proteja a instalação do banco de dados e do host tiebreaker

Para configurações que executam o MetroCluster tiebreaker 1,5 e posterior, você pode proteger e proteger o sistema operacional do host e o banco de dados.

Proteja o host

As diretrizes a seguir mostram como proteger o host onde o software tiebreaker está instalado.

Recomendações de gerenciamento de usuários

- Limite o acesso do usuário "root".
  - Você pode usar usuários capazes de elevar o acesso root para instalar e administrar o software tiebreaker.

- Você pode usar usuários que não são capazes de elevar o acesso root para administrar o software tiebreaker.
- Durante a instalação, você deve criar um grupo chamado "mcctbgrp". O usuário raiz do host e o usuário criado durante a instalação devem ser membros. Somente os membros desse grupo podem administrar totalmente o software tiebreaker.

> Os usuários que não são membros deste grupo não podem acessar o software tiebreaker ou a CLI. Você pode criar usuários adicionais no host e torná-los membros do grupo. Esses membros adicionais não podem administrar totalmente o software tiebreaker. Eles têm acesso ReadOnly e não podem adicionar, alterar ou excluir monitores.

- Não execute tiebreaker como usuário root. Use uma conta de serviço dedicada e sem privilégios para executar o tiebreaker.

- Altere a cadeia de carateres padrão da comunidade no arquivo "/etc/snmp/snmpd.conf".
- Permitir Privileges de escrita mínima. A conta de serviço tiebreaker não deve ter acesso para substituir seu binário executável ou quaisquer arquivos de configuração. Somente diretórios e arquivos para armazenamento de tiebreaker local (por exemplo, para armazenamento de back-end integrado) ou logs de auditoria devem ser graváveis pelo usuário do tiebreaker.
- Não permita usuários anônimos.
  - Defina AllowTcpForwarding como "não" ou use a diretiva Match para restringir usuários anônimos.

Informações relacionadas

- "Documentação do produto Red Hat Enterprise Linux 8"
- "Documentação do produto Red Hat Enterprise Linux 9"
- "Documentação do produto Rocky Linux"

Recomendações de segurança de host de linha de base

- Use criptografia de disco
  - Pode ativar a encriptação de disco. Isso pode ser FullDiskEncryption (hardware), criptografia fornecida pelo Hostos (software) ou pelo host SVM.
- Desative serviços não utilizados que permitam conexões de entrada. Você pode desativar qualquer serviço que não esteja em uso. O software tiebreaker não requer um serviço para conexões de entrada porque todas as conexões da instalação do tiebreaker são enviadas. Os serviços que podem ser ativados por padrão e podem ser desativados são:
  - Servidor HTTP/HTTPS
  - Servidor FTP
  - Telnet, RSH, rlogin
  - Acesso a NFS, CIFS e outros protocolos
  - RDP (RemoteDesktopProtocol), X11 Server, VNC ou outros provedores de serviço "desktop" remotos.

> Você deve deixar o acesso ao console serial (se suportado) ou pelo menos um protocolo habilitado para administrar o host remotamente. Se você desabilitar todos os protocolos, precisará de acesso físico ao host para administração.

- Proteger o host usando FIPS

- Você pode instalar o sistema operacional do host no modo compatível com FIPS e, em seguida, instalar o tiebreaker.

  > O OpenJDK 19 verifica na inicialização se o host está instalado no modo FIPS. Não devem ser necessárias alterações manuais.

- Se você proteger o host, você deve garantir que o host seja capaz de inicializar sem a intervenção do usuário. Se a intervenção do usuário for necessária, a funcionalidade tiebreaker pode não estar disponível se o host for reinicializado inesperadamente. Se isso ocorrer, a funcionalidade tiebreaker só estará disponível após a intervenção manual e quando o host for totalmente inicializado.

- Desative o Histórico de comandos do Shell.
- Atualize com frequência. O tiebreaker é desenvolvido ativamente, e a atualização com frequência é importante para incorporar correções de segurança e quaisquer alterações nas configurações padrão, como comprimentos de chave ou conjuntos de codificação.
- Inscreva-se na lista de discussão do anúncio HashiCorp para receber anúncios de novos lançamentos e visite o CHANGELOG DE tiebreaker para obter detalhes sobre atualizações recentes para novos lançamentos.
- Use as permissões de arquivo corretas. Certifique-se sempre de que as permissões apropriadas sejam aplicadas aos arquivos antes de iniciar o software tiebreaker, especialmente aqueles que contêm informações confidenciais.
- A autenticação multifator (MFA) aumenta a segurança da sua organização, exigindo que os administradores se identifiquem usando mais do que um nome de usuário e senha. Embora importantes, nomes de usuário e senhas são vulneráveis a ataques de força bruta e podem ser roubados por terceiros.
  - O Red Hat Enterprise Linux 8 fornece MFA que exige que os usuários forneçam mais de uma informação para se autenticar com êxito em uma conta ou em um host Linux. As informações adicionais podem ser uma senha única enviada para o seu celular via SMS ou credenciais de um aplicativo como Google Authenticator, Twilio Authy ou FreeOTP.

Informações relacionadas

- "Documentação do produto Red Hat Enterprise Linux 8"
- "Documentação do produto Red Hat Enterprise Linux 9"
- "Documentação do produto Rocky Linux"

Proteja a instalação do banco de dados

As diretrizes a seguir mostram como proteger e proteger a instalação do banco de dados MariaDB 10.x.

- Limite o acesso do usuário "root".
  - Tiebreaker usa uma conta dedicada. A conta e as tabelas para armazenar dados (configuração) são criadas durante a instalação do tiebreaker. O único tempo de acesso elevado ao banco de dados é necessário durante a instalação.
- Durante a instalação são necessários os seguintes acessos e Privileges:
  - A capacidade de criar um banco de dados e tabelas
  - A capacidade de criar opções globais
  - A capacidade de criar um usuário de banco de dados e definir a senha
  - A capacidade de associar o usuário do banco de dados ao banco de dados e tabelas e atribuir direitos de acesso

A conta de usuário especificada durante a instalação do tiebreaker deve ter todos esses Privileges. O uso de várias contas de usuário para as diferentes tarefas não é suportado.

- Use a criptografia do banco de dados
  - A criptografia de dados em repouso é compatível. "Saiba mais sobre criptografia de dados em repouso"
  - Os dados em trânsito não são criptografados. Os dados em voo usam uma conexão de arquivo local "socks".
  - Conformidade FIPS para MariaDB — você não precisa ativar a conformidade FIPS no banco de dados. A instalação do host no modo compatível com FIPS é suficiente.

    "Saiba mais sobre o MySQL Enterprise transparent Data Encryption (TDE)"

As configurações de criptografia devem ser habilitadas antes da instalação do software tiebreaker.

Informações relacionadas

- Gerenciamento de usuários de banco de dados

  "Controle de Acesso e Gerenciamento de conta"

- Proteja o banco de dados

  "Tornando o MySQL seguro contra invasores"

  "Protegendo o MariaDB"

- Proteja a instalação do Vault

  "Endurecimento da produção"

Instale o pacote de software tiebreaker

Escolha o procedimento de instalação

O procedimento de instalação do tiebreaker que você segue depende da versão do tiebreaker que você está instalando.

Versão tiebreaker	Ir para…
Tiebreaker 1,6 ou posterior	"Instale o tiebreaker 1,6 ou posterior"
Desempate 1,5	"Instale o desempate 1,5"
Desempate 1,4	"Instale o desempate 1,4"

Instale o tiebreaker 1,6 ou posterior

Execute uma nova instalação ou atualização para o tiebreaker 1,6 ou tiebreaker 1.6P1 no sistema operacional Linux host para monitorar as configurações do MetroCluster.

Sobre esta tarefa

- O sistema de storage deve estar executando o ONTAP 9.12,1 ou posterior.
- Você pode instalar o tiebreaker do MetroCluster como um usuário não-root com Privileges administrativo suficiente para executar a instalação do tiebreaker, criar tabelas e usuários e definir a senha do usuário.

Instale ou atualize para o tiebreaker 1.6P1

Você pode instalar o tiebreaker 1.6P1 ou atualizar para o tiebreaker 1.6P1 a partir do tiebreaker 1,6, 1,5 ou 1,4.

Passos

1. Baixe o software MetroCluster Tiebreaker 1.6P1.

   "MetroCluster tiebreaker (Downloads) - Site de suporte da NetApp"

2. Faça login no host como usuário raiz.
3. Se você estiver executando uma atualização, verifique a versão do tiebreaker que você está executando:

   O exemplo a seguir mostra o tiebreaker 1,5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Instale ou atualize o software tiebreaker.

Instale o tiebreaker 1.6P1

Siga as etapas a seguir para uma nova instalação do tiebreaker 1.6P1.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para iniciar a instalação:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

O sistema exibe a seguinte saída para uma instalação bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
```

```
                  Mlock: supported: true, enabled: true
          Recovery Mode: false
                Storage: file
                Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
            Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
```

```
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
restored
```

```
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
```

```
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6P1.
```

Atualize 1,6 para 1.6P1

Siga as etapas a seguir para atualizar a versão do software tiebreaker 1,6 para tiebreaker 1.6P1.

> Depois de atualizar para o tiebreaker 1.6P1 do 1,6, remova os monitores existentes e adicione novamente a configuração do MetroCluster para monitoramento.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para atualizar o software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
NetApp-MetroCluster-Tiebreaker-Software-1.6P1-1.x86_64
Error making API request.

URL: GET
https://127.0.0.1:8200/v1/sys/internal/ui/mounts/mcctb/data/db
Code: 403. Errors:

* permission denied
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.19.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.mail-2.0.1.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
```

```
/
chown: missing operand after ‘/var/log/netapp/mcctb’
Try 'chown --help' for more information.
chown: missing operand after ‘/etc/netapp/mcctb’
Try 'chown --help' for more information.
chown: missing operand after ‘/opt/netapp/’
Try 'chown --help' for more information.


Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

b. Remova e adicione novamente a configuração do MetroCluster seguindo as etapas em "Configure o software tiebreaker".

Atualize 1,5 para 1.6P1

Siga as etapas a seguir para atualizar a versão do software tiebreaker 1,5 para tiebreaker 1.6P1.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para atualizar o software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

Atualize 1,4 para 1.6P1

Siga as etapas a seguir para atualizar a versão do software tiebreaker 1,4 para tiebreaker 1.6P1.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para atualizar o software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

Instale ou atualize para o tiebreaker 1,6

Você pode instalar o tiebreaker 1,6 ou atualizar para o tiebreaker 1,6 a partir do tiebreaker 1,5 ou 1,4.

Passos

1. Baixe o software MetroCluster tiebreaker 1,6.

   "MetroCluster tiebreaker (Downloads) - Site de suporte da NetApp"

2. Faça login no host como usuário raiz.
3. Se você estiver executando uma atualização, verifique a versão do tiebreaker que você está executando:

   O exemplo a seguir mostra o tiebreaker 1,5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Instale ou atualize o software tiebreaker.

Instale o desempate 1,6

Siga as etapas a seguir para uma nova instalação do tiebreaker 1,6.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para iniciar a instalação:

```
sh MetroClusterTiebreakerInstall-1.6
```

O sistema exibe a seguinte saída para uma instalação bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
```

```
                  Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
```

```
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
restored
```

```
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
```

```
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6.
```

Atualize 1,5 para 1,6

Siga as etapas a seguir para atualizar a versão do software tiebreaker 1,5 para tiebreaker 1,6.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para atualizar o software:

```
sh MetroClusterTiebreakerInstall-1.6
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Atualize 1,4 para 1,6

Siga as etapas a seguir para atualizar a versão do software tiebreaker 1,4 para tiebreaker 1,6.

Passos

a. Execute o seguinte comando no `[root@mcctb ~] #` prompt para atualizar o software:

```
sh MetroClusterTiebreakerInstall-1.6
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

Exemplo

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Instale o desempate 1,5

Configure o acesso de administrador à API ONTAP e SSH

Você pode configurar o acesso de administrador à API ONTAP e SSH.

Passos

1. Crie um usuário de administrador com acesso à API do ONTAP: `security login create -user-or -group-name` *`mcctb`* `-application ontapi -authentication-method` *`password`*
2. Criar um usuário admin com acesso SSH: `security login create -user-or-group-name` *`mcctb`* `-application` *`ssh`* `-authentication-method` *`password`*
3. Verifique se os novos usuários admin foram criados: `security login show`
4. Repita estas etapas no cluster de parceiros.

> "Autenticação de administrador e RBAC" está implementado.

Instale dependências do MetroCluster tiebreaker 1,5

Dependendo do sistema operacional Linux host, você deve instalar um servidor MySQL

ou MariaDB antes de instalar ou atualizar o software tiebreaker.

Passos

1. Instale o JDK
2. Instale e configure o Vault
3. Instale o servidor MySQL ou MariaDB:

Se o host Linux for	Então…
Red Hat Enterprise Linux 7/CentOS 7	Instale as versões do MySQL Server 5.5.30 ou posterior e 5,6.x no Red Hat Enterprise Linux 7 ou CentOS 7
Red Hat Enterprise Linux 8	Instale o servidor MariaDB no Red Hat Enterprise Linux 8

Instale o JDK

Você deve instalar o JDK em seu sistema host antes de instalar ou atualizar o software tiebreaker. Tiebreaker 1,5 e posterior suporta OpenJDK 17, 18 ou 19.

Passos

1. Faça login como um usuário "root" ou um usuário sudo que pode mudar para o modo de privilégio avançado.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Verifique as versões disponíveis do JDK:

```
yum search openjdk
```

3. Instale o JDK 17,18 ou 19.

   O seguinte comando instala o JDK 17:

```
yum install java-17-openjdk
```

4. Verifique a instalação:

```
java -version
```

   Uma instalação bem-sucedida exibe a seguinte saída:

```
openjdk version "17.0.2" 2022-01-18 LTS
OpenJDK Runtime Environment 21.9 (build 17.0.2+8-LTS)
OpenJDK 64-Bit Server VM 21.9 (build 17.0.2+8-LTS, mixed mode, sharing)
```

Instale e configure o Vault

Se você não tiver ou quiser usar o servidor local do Vault, você deve instalar o Vault. Você pode consultar este procedimento padrão para instalar o Vault ou consultar as instruções de instalação do Hashicorp para obter diretrizes alternativas.

> Se você tiver um servidor do Vault na rede, poderá configurar o host do MetroCluster Tiebreaker para usar essa instalação do Vault. Se você fizer isso, não precisará instalar o Vault no host.

Passos

1. Navegue até o `/bin` diretório:

```
[root@mcctb] cd /bin
```

2. Baixe o arquivo zip do Vault.

```
[root@mcctb /bin]#  curl -sO
https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
```

3. Descompacte o arquivo Vault.

```
[root@mcctb /bin]# unzip vault_1.12.2_linux_amd64.zip
Archive:  vault_1.12.2_linux_amd64.zip
  inflating: vault
```

4. Verifique a instalação.

```
[root@mcctb /bin]# vault -version
Vault v1.12.2 (415e1fe3118eebd5df6cb60d13defdc01aa17b03), built 2022-11-
23T12:53:46Z
```

5. Navegue até o `/root` diretório:

```
[root@mcctb /bin] cd /root
```

6. Crie um arquivo de configuração do Vault sob o `/root` diretório.

```
`[root@mcctb ~]`No prompt, copie e execute o seguinte comando para criar
o `config.hcl` arquivo:
```

```
# cat > config.hcl << EOF
 storage "file" {
  address = "127.0.0.1:8500"
  path    = "/mcctb_vdata/data"
 }
 listener "tcp" {
   address     = "127.0.0.1:8200"
   tls_disable = 1
 }
EOF
```

7. Inicie o servidor Vault:

```
[root@mcctb ~] vault server -config config.hcl &
```

8. Exporte o endereço do Vault.

```
[root@mcctb ~]# export VAULT_ADDR="http://127.0.0.1:8200"
```

9. Inicialize o Vault.

```
[root@mcctb ~]# vault operator init
2022-12-15T14:57:22.113+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.113+0530 [INFO]  core: seal configuration missing,
not initialized
2022-12-15T14:57:22.114+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.116+0530 [INFO]  core: security barrier initialized:
stored=1 shares=5 threshold=3
2022-12-15T14:57:22.118+0530 [INFO]  core: post-unseal setup starting
2022-12-15T14:57:22.137+0530 [INFO]  core: loaded wrapping token key
2022-12-15T14:57:22.137+0530 [INFO]  core: Recorded vault version: vault
version=1.12.2 upgrade time="2022-12-15 09:27:22.137200412 +0000 UTC"
build date=2022-11-23T12:53:46Z
2022-12-15T14:57:22.137+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T14:57:22.137+0530 [INFO]  core: no mounts; adding default
mount table
2022-12-15T14:57:22.143+0530 [INFO]  core: successfully mounted backend:
type=cubbyhole version="" path=cubbyhole/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=system version="" path=sys/
```

```
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=identity version="" path=identity/
2022-12-15T14:57:22.148+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T14:57:22.149+0530 [INFO]  rollback: starting rollback manager
2022-12-15T14:57:22.149+0530 [INFO]  core: restoring leases
2022-12-15T14:57:22.150+0530 [INFO]  expiration: lease restore complete
2022-12-15T14:57:22.150+0530 [INFO]  identity: entities restored
2022-12-15T14:57:22.150+0530 [INFO]  identity: groups restored
2022-12-15T14:57:22.151+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T14:57:23.385+0530 [INFO]  core: post-unseal setup complete
2022-12-15T14:57:23.387+0530 [INFO]  core: root token generated
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown starting
2022-12-15T14:57:23.387+0530 [INFO]  rollback: stopping rollback manager
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown complete
Unseal Key 1: <unseal_key_1_id>
Unseal Key 2: <unseal_key_2_id>
Unseal Key 3: <unseal_key_3_id>
Unseal Key 4: <unseal_key_4_id>
Unseal Key 5: <unseal_key_5_id>

Initial Root Token: <initial_root_token_id>


Vault initialized with 5 key shares and a key threshold of 3. Please
securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to
unseal it
before it can start servicing requests.

Vault does not store the generated root key. Without at least 3 keys to
reconstruct the root key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum
of
existing unseal keys shares. See "vault operator rekey" for more
information.
```

Você deve gravar e armazenar os IDs de chave e o token de raiz inicial em um local seguro para uso posterior no procedimento.

10. Exporte o token raiz do Vault.

```
[root@mcctb ~]#  export VAULT_TOKEN="<initial_root_token_id>"
```

11. Desprenda o Vault usando quaisquer três das cinco chaves que foram criadas.

    Você deve executar o `vault operator unseal` comando para cada uma das três chaves:

    a. Retire o Vault usando a primeira chave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    1/3
Unseal Nonce       <unseal_key_1_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

    b. Retire o Vault usando a segunda chave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    2/3
Unseal Nonce       <unseal_key_2_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

    c. Retire o Vault usando a terceira chave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=127.0.0.1:8201
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener: serving
cluster requests: cluster_listen_address=127.0.0.1:8201
2022-12-15T15:15:00.981+0530 [INFO]  core: post-unseal setup starting
2022-12-15T15:15:00.981+0530 [INFO]  core: loaded wrapping token key
2022-12-15T15:15:00.982+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T15:15:00.983+0530 [INFO]  core: successfully mounted
backend: type=system version="" path=sys/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=identity version="" path=identity/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=cubbyhole version="" path=cubbyhole/
2022-12-15T15:15:00.986+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T15:15:00.986+0530 [INFO]  rollback: starting rollback
manager
2022-12-15T15:15:00.987+0530 [INFO]  core: restoring leases
2022-12-15T15:15:00.987+0530 [INFO]  expiration: lease restore
complete
2022-12-15T15:15:00.987+0530 [INFO]  identity: entities restored
2022-12-15T15:15:00.987+0530 [INFO]  identity: groups restored
2022-12-15T15:15:00.988+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T15:15:00.989+0530 [INFO]  core: post-unseal setup complete
2022-12-15T15:15:00.989+0530 [INFO]  core: vault is unsealed
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

12. Verifique se o status do Vault selado é falso.

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

13. Configure o serviço Vault para iniciar na inicialização.
    a. Execute o seguinte comando: `cd /etc/systemd/system`

    ```
    [root@mcctb ~]#  cd /etc/systemd/system
    ```

    b. `[root@mcctb system]`No prompt, copie e execute o seguinte comando para criar o arquivo de serviço do Vault.

    ```
    # cat > vault.service << EOF
    [Unit]
    Description=Vault Service
    After=mariadb.service

    [Service]
    Type=forking
    ExecStart=/usr/bin/vault server -config /root/config.hcl &
    Restart=on-failure

    [Install]
    WantedBy=multi-user.target
    EOF
    ```

    c. Execute o seguinte comando: `systemctl daemon-reload`

    ```
    [root@mcctb system]#  systemctl daemon-reload
    ```

    d. Execute o seguinte comando: `systemctl enable vault.service`

```
[root@mcctb system]#  systemctl enable vault.service
Created symlink /etc/systemd/system/multi-
user.target.wants/vault.service → /etc/systemd/system/vault.service.
```

Você será solicitado a usar esse recurso durante a instalação do MetroCluster Tiebreaker. Se você quiser alterar o método para desselar o Vault, então você precisa desinstalar e reinstalar o software tiebreaker do MetroCluster.

Instale as versões do MySQL Server 5.5.30 ou posterior e 5,6.x no Red Hat Enterprise Linux 7 ou CentOS 7

Você deve instalar o MySQL Server 5.5.30 ou posterior e a versão 5,6.x no sistema host antes de instalar ou atualizar o software tiebreaker. Para Red Hat Enterprise Linux 8, Instale o servidor MariaDB.

Passos

1. Faça login como um usuário raiz ou um usuário sudo que pode mudar para o modo de privilégio avançado.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Adicione o repositório MySQL ao seu sistema host:

```
[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
========
Package               Arch   Version
                                    Repository
Size
================================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
================================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Desative o repositório MySQL 57:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Ative o repositório MySQL 56:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Ativar o repositório:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Instale o servidor da Comunidade MySQL:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
======
Package                          Arch   Version       Repository
Size
================================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 --------------------------------------------------------------------------
--------
Total                                                289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. Inicie o servidor MySQL:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Confirme se o servidor MySQL está em execução:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Configurar definições de segurança e palavra-passe:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                        hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Verifique se o login do MySQL está funcionando:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Se o login do MySQL estiver funcionando, a saída terminará no `mysql>` prompt.

Ative a configuração de inicialização automática do MySQL

Você deve verificar se o recurso autostart está ativado para o daemon MySQL. Ativar o daemon MySQL reinicia automaticamente o MySQL se o sistema no qual o software tiebreaker do MetroCluster reside for reinicializado. Se o daemon MySQL não estiver em execução, o software tiebreaker continua em execução, mas não pode ser reiniciado e as alterações de configuração não podem ser feitas.

Passo

1. Verifique se o MySQL está habilitado para iniciar automaticamente quando inicializado:

```
[root@mcctb ~]# systemctl list-unit-files mysqld.service
```

```
UNIT FILE          State
------------------ ----------
mysqld.service     enabled
```

Se o MySQL não estiver habilitado para iniciar automaticamente quando inicializado, consulte a documentação do MySQL para ativar o recurso de inicialização automática para sua instalação.

Instale o servidor MariaDB no Red Hat Enterprise Linux 8

Você deve instalar o servidor MariaDB no sistema host antes de instalar ou atualizar o software tiebreaker. Para Red Hat Enterprise Linux 7 ou CentOS 7, Instale o MySQL Server.

Antes de começar

Seu sistema host deve estar em execução no Red Hat Enterprise Linux (RHEL) 8.

Passos

1. Faça login como um `root` usuário ou um usuário que pode sudo para o modo de privilégio avançado.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Instale o servidor MariaDB:

```
[root@mcctb ~]# yum install mariadb-server.x86_64
```

```
[root@mcctb ~]# yum install mariadb-server.x86_64
Loaded plugins: fastestmirror, langpacks
 ...
 ...

================================================================================
===
 Package                       Arch    Version         Repository
Size
================================================================================
===
Installing:
mariadb-server                x86_64   1:5.5.56-2.el7   base
11 M
```

```
Installing for dependencies:

Transaction Summary
================================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
--------------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. Inicie o servidor MariaDB:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Verifique se o servidor MariaDB foi iniciado:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Configure as definições de segurança e palavra-passe:

> Quando for solicitada a palavra-passe raiz, deixe-a vazia e prima ENTER para continuar a configurar as definições de segurança e palavra-passe.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
```

```
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Ative a configuração de início automático para o servidor MariaDB

Você deve verificar se o recurso de inicialização automática está ativado para o servidor MariaDB. Se você não ativar o recurso de inicialização automática e o sistema no qual o software tiebreaker do MetroCluster reside precisar reinicializar, o software tiebreaker continuará em execução, mas o serviço MariaDB não poderá ser reiniciado e as alterações de configuração não poderão ser feitas.

Passos

1. Ative o serviço de arranque automático:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Verifique se o MariaDB está habilitado para iniciar automaticamente quando inicializado:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Instale ou atualize para o tiebreaker 1,5

Execute uma nova instalação ou atualização para o tiebreaker 1,5 no sistema operacional Linux host para monitorar as configurações do MetroCluster.

Sobre esta tarefa

- Seu sistema de storage deve estar executando uma versão compatível do ONTAP. Consulte "Requisitos de software"a tabela para obter mais detalhes.
- Você deve ter instalado o OpenJDK usando o `yum install java-x.x.x-openjdk` comando. Tiebreaker 1,5 e posterior suporta OpenJDK 17, 18 ou 19.
- Você pode instalar o tiebreaker do MetroCluster como um usuário não-root com Privileges administrativo suficiente para executar a instalação do tiebreaker, criar tabelas e usuários e definir a senha do usuário.

Passos

1. Baixe o software tiebreaker do MetroCluster e a chave MetroCluster_tiebreaker_RPM_GPG.

   A chave MetroCluster_tiebreaker_RPM_GPG está disponível para download na mesma página que você faz o download do pacote de software para tiebreaker 1,5 no site de suporte da NetApp.

   "MetroCluster tiebreaker (Downloads) - Site de suporte da NetApp"

2. Faça login no host como usuário raiz.
3. Crie um usuário não-root e o `mcctbgrp` grupo.

   a. Crie um usuário que não seja root e defina a senha.

      Os comandos de exemplo a seguir criam um usuário não-root chamado `mcctbuser1`:

      ```
      [root@mcctb ~]# useradd mcctbuser1
      [root@mcctb ~]# passwd mcctbuser1
      Changing password for user mcctbuser1.
      New password:
      Retype new password:
      passwd: all authentication tokens updated successfully.
      ```

   b. Criar um grupo chamado `mcctbgrp`:

```
[root@mcctb ~~]# groupadd mcctbgrp
```

c. Adicione o usuário não-root que você criou ao `mcctbgrp` grupo.

O seguinte comando é adicionado `mcctbuser1` ao `mcctbgrp` grupo:

```
[root@mcctb ~]# usermod -a -G mcctbgrp mcctbuser1
```

4. Verifique o arquivo RPM.

Execute as seguintes subetapas a partir do diretório que contém a chave RPM.

a. Baixe e importe o arquivo de chave RPM:

```
[root@mcctb ~]# rpm --import MetroCluster_Tiebreaker_RPM_GPG.key
```

b. Verifique se a chave correta foi importada verificando a impressão digital.

O exemplo a seguir mostra uma impressão digital chave correta:

```
root@mcctb:~/signing/mcctb-rpms# gpg --show-keys --with-fingerprint
MetroCluster_Tiebreaker_RPM_GPG.key
pub   rsa3072 2022-11-17 [SCEA] [expires: 2025-11-16]
      65AC 1562 E28A 1497 7BBD  7251 2855 EB02 3E77 FAE5
uid                      MCCTB-RPM (mcctb RPM production signing)
<mcctb-rpm@netapp.com>
```

a. Verifique a assinatura: `rpm --checksig NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

```
NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm: digests OK
```

Só tem de prosseguir com a instalação depois de ter verificado com êxito a assinatura.

5. instale ou atualize o software tiebreaker:

Você só pode atualizar para a versão 1,5 do tiebreaker quando estiver atualizando a partir da versão 1,4 do tiebreaker. A atualização de versões anteriores para o tiebreaker 1,5 não é suportada.

Selecione o procedimento correto dependendo se você está executando uma nova instalação ou atualizando uma instalação existente.

Execute uma nova instalação

a. Recuperar e gravar o caminho absoluto para Java:

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Execute o seguinte comando:
`rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

O sistema exibe a seguinte saída para uma instalação bem-sucedida:

> Quando solicitado durante a instalação, forneça o usuário não-root que você criou e atribuiu anteriormente ao `mcctbgrp` grupo.

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Enter database user name:
root
Please enter database password for root
Enter password:
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.5.
```

Atualizando uma instalação existente

a. Verifique se uma versão suportada do OpenJDK está instalada e se é a versão atual do Java localizada no host.

> Para atualizações para o tiebreaker 1,5, você deve instalar o OpenJDK versão 17, 18 ou 19.

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Verifique se o serviço Vault está deslacado e em execução: `vault status`

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault
Cluster ID      <cluster_id>
HA Enabled      false
```

c. Atualize o software tiebreaker.

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.5-1.x86_64.rpm
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]

Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Enter database user name : root
Please enter database password for root
Enter password:
Password updated successfully in the database.
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.5.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Se você digitar a senha raiz errada do MySQL, o software tiebreaker indica que ele foi instalado com sucesso, mas exibe mensagens "Acesso negado". Para resolver o problema, você deve desinstalar o software tiebreaker usando o `rpm -e` comando e reinstalar o software usando a senha raiz do MySQL correta.

6. Verifique a conetividade tiebreaker com o software MetroCluster abrindo uma conexão SSH do host tiebreaker para cada uma das LIFs de gerenciamento de nós e LIFs de gerenciamento de cluster.

Informações relacionadas

"Suporte à NetApp"

Instale o desempate 1,4

Instale dependências do MetroCluster tiebreaker 1,4

Dependendo do sistema operacional Linux host, instale um servidor MySQL ou MariaDB antes de instalar ou atualizar o software tiebreaker.

Passos

1. Instale o JDK.
2. Instale o servidor MySQL ou MariaDB:

Se o host Linux for	Então…
Red Hat Enterprise Linux 7/CentOS 7	Instale as versões do MySQL Server 5.5.30 ou posterior e 5,6.x no Red Hat Enterprise Linux 7 ou CentOS 7
Red Hat Enterprise Linux 8	Instale o servidor MariaDB no Red Hat Enterprise Linux 8

Instale o JDK

Você deve instalar o JDK em seu sistema host antes de instalar ou atualizar o software tiebreaker. O tiebreaker 1,4 e anterior suporta JDK 1,8.0. (JRE 8).

Passos

1. Faça login como um usuário "root".

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Instale o JDK 1,8.0:

```
yum install java-1.8.0-openjdk.x86_64
```

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

================================================================================
Package               Arch   Version                 Repository    Size
================================================================================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4 updates      238 k
 ..
 ..
Transaction Summary
================================================================================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Instale as versões do MySQL Server 5.5.30 ou posterior e 5,6.x no Red Hat Enterprise Linux 7 ou CentOS 7

Você deve instalar o MySQL Server 5.5.30 ou posterior e a versão 5,6.x no sistema host antes de instalar ou atualizar o software tiebreaker. Para Red Hat Enterprise Linux 8, Instale o servidor MariaDB.

Passos

1. Faça login como usuário root.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Adicione o repositório MySQL ao seu sistema host:

```
[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
========
Package               Arch   Version
                                    Repository
Size
================================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
================================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Desative o repositório MySQL 57:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Ative o repositório MySQL 56:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Ativar o repositório:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Instale o servidor da Comunidade MySQL:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
================================================================================
======
Package                          Arch   Version       Repository
Size
================================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ------------------------------------------------------------------------
--------
Total                                              289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. Inicie o servidor MySQL:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Confirme se o servidor MySQL está em execução:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Configurar definições de segurança e palavra-passe:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                        hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Verifique se o login do MySQL está funcionando:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Quando o login do MySQL está funcionando como esperado, a saída termina `mysql>` no prompt.

Ative a configuração de inicialização automática do MySQL

Você deve verificar se o recurso autostart está ativado para o daemon MySQL. Ativar o daemon MySQL reinicia automaticamente o MySQL se o sistema no qual o software tiebreaker do MetroCluster reside for reinicializado. Se o daemon MySQL não estiver em execução, o software tiebreaker continua em execução, mas não pode ser reiniciado e as alterações de configuração não podem ser feitas.

Passo

1. Verifique se o MySQL está habilitado para iniciar automaticamente quando inicializado:

```
[root@mcctb ~]# systemctl list-unit-files mysqld.service
```

```
UNIT FILE          State
------------------ ----------
mysqld.service     enabled
```

Se o MySQL não estiver habilitado para iniciar automaticamente quando inicializado, consulte a documentação do MySQL para ativar o recurso de inicialização automática para sua instalação.

Instale o servidor MariaDB no Red Hat Enterprise Linux 8

Você deve instalar o servidor MariaDB no sistema host antes de instalar ou atualizar o software tiebreaker. Para Red Hat Enterprise Linux 7 ou CentOS 7, Instale o MySQL Server.

Antes de começar

Seu sistema host deve estar em execução no Red Hat Enterprise Linux (RHEL) 8.

Passos

1. Inicie sessão como `root` utilizador.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Instale o servidor MariaDB:

```
[root@mcctb ~]# yum install mariadb-server.x86_64
```

```
[root@mcctb ~]# yum install mariadb-server.x86_64
Loaded plugins: fastestmirror, langpacks
 ...
 ...

================================================================================
===
 Package                       Arch    Version         Repository
Size
================================================================================
===
Installing:
mariadb-server                x86_64   1:5.5.56-2.el7   base
11 M
```

```
Installing for dependencies:

Transaction Summary
================================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
--------------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. Inicie o servidor MariaDB:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Verifique se o servidor MariaDB foi iniciado:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Configure as definições de segurança e palavra-passe:

> Quando for solicitada a palavra-passe raiz, deixe-a vazia e prima ENTER para continuar a configurar as definições de segurança e palavra-passe.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
```

```
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

  ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Ative a configuração de início automático para o servidor MariaDB

Você deve verificar se o recurso de inicialização automática está ativado para o servidor MariaDB. Se você não ativar o recurso de inicialização automática e o sistema no qual o software tiebreaker do MetroCluster reside precisar reinicializar, o software tiebreaker continuará em execução, mas o serviço MariaDB não poderá ser reiniciado e as alterações de configuração não poderão ser feitas.

Passos

1. Ative o serviço de arranque automático:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Verifique se o MariaDB está habilitado para iniciar automaticamente quando inicializado:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Instale ou atualize para o tiebreaker 1,4

Execute uma nova instalação ou atualização para o tiebreaker 1,4 no sistema operacional Linux host para monitorar as configurações do MetroCluster.

Sobre esta tarefa

- Seu sistema de storage deve estar executando uma versão compatível do ONTAP. Consulte "Requisitos de software"a tabela para obter mais detalhes.
- Você deve ter instalado o OpenJDK usando o `yum install java-x.x.x-openjdk` comando. O tiebreaker 1,4 e anterior suporta JDK 1.8.0 (JRE 8).

Passos

1. Baixe o software tiebreaker do MetroCluster.

   "MetroCluster tiebreaker (Downloads) - Site de suporte da NetApp"

2. Faça login no host como usuário raiz.
3. instale ou atualize o software tiebreaker:

   Selecione o procedimento correto dependendo se você está executando uma nova instalação ou atualizando uma instalação existente.

Execute uma nova instalação

a. Instale o software tiebreaker executando o :

```
rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.4-1.x86_64.rpm
```

O sistema exibe a seguinte saída para uma instalação bem-sucedida:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Post installation start Fri Apr  5 02:28:09 EDT 2024
Enter MetroCluster Tiebreaker user password:

Please enter mysql root password when prompted
Enter password:
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post installation end Fri Apr  5 02:28:22 EDT 2024
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.4.
```

Atualizar uma instalação existente

a. Atualize o software tiebreaker.

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.4-1.x86_64.rpm
```

O sistema exibe a seguinte saída para uma atualização bem-sucedida:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Upgrading NetApp MetroCluster Tiebreaker software....
Stopping NetApp MetroCluster Tiebreaker software services before
upgrade.
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Post installation start Mon Apr  8 06:29:51 EDT 2024
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post upgrade end Mon Apr  8 06:29:51 EDT 2024
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.4.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Se você digitar a senha raiz errada do MySQL, o software tiebreaker indica que ele foi instalado com sucesso, mas exibe mensagens "Acesso negado". Para resolver o problema, você deve desinstalar o software tiebreaker usando o `rpm -e` comando e reinstalar o software usando a senha raiz do MySQL correta.

4. Verifique a conetividade tiebreaker com o software MetroCluster abrindo uma conexão SSH do host tiebreaker para cada uma das LIFs de gerenciamento de nós e LIFs de gerenciamento de cluster.

Informações relacionadas

"Suporte à NetApp"

Atualize o host onde o monitor tiebreaker está sendo executado

Talvez seja necessário atualizar o host no qual o monitor tiebreaker está sendo executado.

Passos

1. Desinstale o software tiebreaker:

   ```
   rpm -e NetApp-MetroCluster-Tiebreaker-Software
   ```

2. Atualize o host. Consulte a documentação do sistema operacional do host para obter detalhes.
3. Reinstale o software tiebreaker.

   Execute uma nova instalação do tiebreaker seguindo as etapas em "Instale o software tiebreaker".

Configurando o software tiebreaker

Após a instalação do software tiebreaker, você pode adicionar ou modificar configurações do MetroCluster ou removê-las do software tiebreaker.

Iniciar a CLI do software tiebreaker

Depois de instalar o software tiebreaker, você deve iniciar sua CLI para configurar o software.

1. Inicie a CLI a partir do prompt do host no qual você instalou o software:

   ```
   netapp-metrocluster-tiebreaker-software-cli
   ```

2. Após a instalação e durante a primeira inicialização, digite a senha para o usuário tiebreaker acessar o banco de dados. Esta é a senha que você especificou para o usuário do banco de dados durante a instalação.

Adição de configurações do MetroCluster

Depois de instalar o software tiebreaker do NetApp MetroCluster, você pode adicionar mais configurações do MetroCluster, uma de cada vez.

Você deve ter instalado a configuração do MetroCluster em um ambiente ONTAP e ativado as configurações no software.

1. Use o comando add do monitor da interface de linha de comando (CLI) tiebreaker para adicionar configurações do MetroCluster.

   Se você estiver usando o nome do host, ele deve ser o nome de domínio totalmente qualificado (FQDN).

   O exemplo a seguir mostra a configuração de cluster_A:

```
NetApp MetroCluster Tiebreaker :> monitor add wizard
Enter monitor Name: cluster_A
Enter Cluster IP Address: 10.222.196.130
Enter Cluster Username: admin
Enter Cluster Password:
Enter Peer Cluster IP Address: 10.222.196.40
Enter Peer Cluster Username: admin
Enter Peer Cluster Password:
Successfully added monitor to NetApp MetroCluster Tiebreaker software.
```

2. Confirme se a configuração do MetroCluster foi adicionada corretamente usando o comando tiebreaker CLI `monitor show -status`.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

3. Desative o modo observador para que o software tiebreaker inicie automaticamente um switchover após detetar uma falha no local:

   `monitor modify -monitor-name monitor_name -observer-mode false`

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
-observer-mode false
Warning: If you are turning observer-mode to false, make sure to review
the 'risks and limitations'
as described in the MetroCluster Tiebreaker installation and
configuration.
Are you sure you want to enable automatic switchover capability for
monitor "8pack"? [Y/N]: y
```

Informações relacionadas

"Riscos e limitações do uso do MetroCluster Tiebreaker no modo ativo"

Comandos para modificar configurações do MetroCluster tiebreaker

Você pode modificar a configuração do MetroCluster sempre que precisar alterar as configurações.

O comando tiebreaker CLI monitor Modify pode ser usado com qualquer uma das seguintes opções. Você pode confirmar suas alterações com o comando monitor show -status.

Opção	Descrição
-monitor-name	Nome da configuração do MetroCluster
-enable-monitor	Ativa e desativa a monitorização da configuração do MetroCluster

-período silencioso	Período em segundos pelo qual o software tiebreaker do MetroCluster aguarda para confirmar uma falha do local após a deteção
-modo observador	O modo observador (verdadeiro) fornece apenas monitoramento e não aciona um switchover se ocorrer um desastre no local. O modo online (false) aciona um switchover se ocorrer um desastre no local. • "Como o software tiebreaker deteta falha no local" • "Riscos e limitações do uso do MetroCluster Tiebreaker no modo ativo"

O exemplo a seguir altera o período silencioso para a configuração.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

O comando tiebreaker CLI `debug` pode ser usado para alterar o modo de Registro.

Comando	Descrição
status de depuração	Exibe o status do modo de depuração
ativar depuração	Ativa o modo de depuração para o registo
desativar depuração	Desativa o modo de depuração para o registo

Em sistemas que executam o tiebreaker 1,4 e anteriores, o comando tiebreaker CLI `update-mcctb-password` pode ser usado para atualizar a senha do usuário. Este comando está obsoleto no tiebreaker 1,5 e posterior.

Comando	Descrição
update-mcctb-password	A palavra-passe do utilizador foi atualizada com êxito

Remoção das configurações do MetroCluster

Você pode remover a configuração do MetroCluster que está sendo monitorada pelo software tiebreaker quando não quiser mais monitorar uma configuração do MetroCluster.

1. Use o comando tiebreaker CLI `monitor remove` para remover a configuração do MetroCluster.

   No exemplo a seguir, "'cluster_A" é removido do software:

```
NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
Successfully removed monitor from NetApp MetroCluster Tiebreaker
software.
```

2. Confirme se a configuração do MetroCluster foi removida corretamente usando o comando tiebreaker CLI `monitor show -status`.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

Configurando as configurações SNMP para o software tiebreaker

Para utilizar o SNMP com o software tiebreaker, tem de configurar as definições SNMP.

Sobre esta tarefa

- O tiebreaker 1,6 só suporta SNMPv3.
- Embora o tiebreaker 1,5 e 1,4 suportem SNMPv1 e SNMPv3, a NetApp recomenda fortemente que você configure o SNMPv3 para uma segurança ideal.

Passos

1. Use o comando tiebreaker CLI `snmp config wizard` para adicionar configurações do MetroCluster.

   Apenas um host de trap SNMP é suportado atualmente.

   A `snmp config wizard` resposta do comando depende da versão do tiebreaker que você está executando.

Desempate 1,6

O exemplo a seguir mostra a configuração de um recetor SNMP que suporta SNMPv3 com um endereço IP de 192.0.2.255 e número de porta 162 para mensagens de intercetação. O software tiebreaker está pronto para enviar traps para o recetor SNMP que você especificou.

O tiebreaker 1,6 só suporta SNMPv3

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
```

Desempate 1,5 e 1,4

O exemplo a seguir mostra a configuração de um recetor SNMP que suporta SNMPv3 com um endereço IP de 192.0.2.255 e número de porta 162 para mensagens de intercetação. O software tiebreaker está pronto para enviar traps para o recetor SNMP que você especificou.

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Version[V1/V3]: v3
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
Enter SNMP V3 Privacy password:
Engine ID : 8000031504932eff571825192a6f1193b265e24593
Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
software.
```

Você deve configurar o SNMPv3 porque o SNMPv1 não é seguro. Verifique se a string de comunidade padrão é **not** definida como public.

2. Verifique se as definições SNMP estão configuradas:

   `snmp config test`

   O exemplo a seguir mostra que o software tiebreaker pode enviar uma armadilha SNMP para o evento TEST_SNMP_CONFIG:

```
NetApp MetroCluster Tiebreaker :> snmp config test
Sending SNMP trap to localhost. Version : V3.
Successfully sent SNMP trap for event TEST_SNMP_CONFIG
NetApp MetroCluster Tiebreaker :>
```

Monitorização da configuração do MetroCluster

O software tiebreaker do MetroCluster automatiza o processo de recuperação, permitindo que você monitore o status da configuração do MetroCluster, avalie os eventos e traps SNMP enviados ao suporte ao cliente do NetApp e visualize o status das operações de monitoramento.

Configurando o AutoSupport

Por padrão, as mensagens AutoSupport são enviadas para o NetApp uma semana após a instalação do software tiebreaker. Os eventos que acionam a notificação do AutoSupport incluem panics do software tiebreaker, detecção de condições de desastre em configurações do MetroCluster ou um status de configuração desconhecido do MetroCluster.

Antes de começar

Você deve ter acesso direto para configurar mensagens do AutoSupport.

Passos

1. Use o comando tiebreaker CLI AutoSupport com qualquer uma das seguintes opções:

Opção	Descrição
-invocar	Envia uma mensagem AutoSupport ao suporte ao cliente
-configure o assistente	Assistente para configurar credenciais do servidor proxy
-eliminar configuração	Exclui as credenciais do servidor proxy
--ativar	Ativa a notificação AutoSupport (esta é a predefinição.)
-disable	Desativa a notificação AutoSupport
-show	Exibe o status do AutoSupport

O exemplo a seguir mostra que o AutoSupport está ativado ou desativado e o destino para o qual o conteúdo do AutoSupport é publicado:

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status            : disabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status            : enabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission      : success
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

O exemplo a seguir mostra o AutoSupport configurado por meio de um servidor proxy autenticado, usando um endereço IP e um número de porta:

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

O exemplo a seguir mostra a exclusão de uma configuração do AutoSupport:

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

Eventos e traps SNMP

O software tiebreaker NetApp MetroCluster usa traps SNMP para notificá-lo de eventos significativos. Esses traps fazem parte do arquivo MIB do NetApp. Cada armadilha contém as seguintes informações: Nome da armadilha, gravidade, nível de impactos, carimbo de data/hora e mensagem.

Nome do evento	Detalhe do evento	Número de armadilha
O disjuntor MetroCluster não consegue alcançar a configuração do MetroCluster	Avisa o administrador de que o software não consegue detetar um desastre. Este evento ocorre quando ambos os clusters não são alcançáveis.	25000
O disjuntor MetroCluster não consegue alcançar o cluster	Avisa o administrador de que o software não pode alcançar um dos clusters.	25001
O disjuntor de ligação MetroCluster detetou um desastre no cluster	Notifica o administrador de que o software deteta uma falha no local. Uma notificação será entregue.	25002
Todos os links entre o cluster de parceiros são cortados.	O software deteta que ambos os clusters estão acessíveis, mas todos os caminhos de rede entre os dois clusters estão inativos e os clusters não podem se comunicar entre si.	25005
Intercetação de teste SNMP	A configuração SNMP agora pode ser testada executando o comando snmp config test.	25006

Apresentar o estado das operações de monitorização

Você pode exibir o status geral das operações de monitoramento para uma configuração do MetroCluster.

Passo

1. Use o comando show do monitor da CLI tiebreaker para exibir o status de uma operação do MetroCluster com qualquer uma das seguintes opções:

Opção	Descrição
-monitor-name	Exibe o status do nome do monitor especificado
-operação-história	Exibe até 10 operações de monitoramento que foram executadas pela última vez em um cluster
-stats	Apresenta as estatísticas relacionadas com o cluster especificado
-status	Exibe o status do cluster especificado **Observação:** o software tiebreaker do MetroCluster pode levar até 10 minutos para refletir o status de conclusão de operações como heal agregados, heal roots ou switchback.

   O exemplo a seguir mostra que os clusters cluster_A e cluster_B estão conetados e íntegros:

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

No exemplo a seguir, as últimas sete operações que foram executadas no cluster_B são exibidas:

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

Exibindo informações de configuração do MetroCluster

Você pode exibir o nome do monitor e o endereço IP de todas as instâncias de configurações do MetroCluster no software tiebreaker.

Passo

1. Use o comando tiebreaker CLI Configuration show para exibir as informações de configuração do MetroCluster.

   O exemplo a seguir mostra as informações dos clusters cluster_A e cluster_B:

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

Criando arquivos de despejo

Você salva o status geral do software tiebreaker em um arquivo de despejo para fins de depuração.

Passo

1. Use o comando tiebreaker CLI monitor dump -status para criar um arquivo de despejo do status geral de todas as configurações do MetroCluster.

   O exemplo a seguir mostra a criação bem-sucedida do arquivo de despejo /var/log/NetApp/mcctb/MetroCluster-tiebreaker-status.xml:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

Riscos e limitações do uso do MetroCluster Tiebreaker no modo ativo

O switchover na deteção de uma falha no local acontece automaticamente, com o MetroCluster Tiebreaker no modo ativo. Este modo pode ser utilizado para complementar a capacidade de comutação automática ONTAP/FAS.

Quando você implementa o tiebreaker do MetroCluster no modo ativo, os seguintes problemas conhecidos podem levar à perda de dados:

- Quando o link entre sites falha, os controladores em cada site continuam a atender os clientes. No entanto, os controladores não serão espelhados. A falha de um controlador em um local é identificada como uma falha no local e o tiebreaker do MetroCluster inicia um switchover. Os dados que não são espelhados após a falha do link entre sites com o local remoto serão perdidos.
- Um switchover ocorre quando os agregados em local remoto estão em estado degradado. Os dados não serão replicados se o switchover tiver ocorrido antes da ressincronização agregada.
- Ocorre uma falha de storage remoto quando o switchover está em andamento.
- A memória não volátil (NVRAM ou NVMEM, dependendo do modelo da plataforma) nas controladoras de storage não é espelhada para o parceiro de recuperação de desastres (DR) remota no local do parceiro.
- Os metadados são perdidos se a rede de peering de cluster estiver inativa por um período prolongado e os volumes de metadados não estiverem online após um switchover.

Você pode encontrar cenários que não são mencionados. A NetApp não é responsável por quaisquer danos que possam surgir fora do uso do MetroCluster Tiebreaker no modo ativo. Não use o tiebreaker do MetroCluster no modo ativo se os riscos e limitações não forem aceitáveis para você.

Requisitos de firewall para desempate do MetroCluster

O tiebreaker do MetroCluster usa várias portas para se comunicar com serviços específicos.

A tabela a seguir lista as portas que você deve permitir no firewall:

Porta/serviços	Fonte	Destino	Finalidade
443 / TCP	Desempate	Internet	Enviando mensagens AutoSupport para o NetApp

22 / TCP	Host de gerenciamento	Desempate	Gerenciamento de desempate
443 / TCP	Desempate	LIFs de gerenciamento de clusters	Comunicações seguras para cluster via HTTP (SSL)
22 / TCP	Desempate	LIFs de gerenciamento de clusters	Comunicações seguras para cluster via SSH
443 / TCP	Desempate	LIFs de gerenciamento de nós	Comunicações seguras para nó via HTTP (SSL)
22 / TCP	Desempate	LIFs de gerenciamento de nós	Comunicações seguras para nó via SSH
162 / UDP	Desempate	Host de trap SNMP	Usado para enviar armadilhas SNMP de notificação de alerta
ICMP (ping)	Desempate	LIFs de gerenciamento de clusters	Verifique se o IP do cluster está acessível
ICMP (ping)	Desempate	LIFs de gerenciamento de nós	Verifique se o IP do nó está acessível

Arquivos de log de eventos para MetroCluster tiebreaker

O arquivo de log de eventos contém um log de todas as ações executadas pelo software tiebreaker do MetroCluster.

O software tiebreaker executa as seguintes ações:

- Detecta desastres no local
- Detecta alterações de configuração relacionadas ao banco de dados, a outros monitores tiebreaker ou ao software tiebreaker MetroCluster
- Detecta conexões SSH e desconexões
- Descobre configurações do MetroCluster

Essas ações são registradas no arquivo de log de eventos no seguinte formato:

<timestamp> (gravidade/nível de registo)> <thread-id> <module>

```
2022-09-07 06:14:30,797 INFO  [MCCTBCommandServer-16] [SslSupport]
Successfully initiated SSL context. Protocol used is TLSv1.3.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16] [DataBase]
Successfully read MCCTB database.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16]
[ConfigurationMonitor] Debug mode disabled.
```

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Documentação do MetroCluster"	• Todas as informações do MetroCluster
"Relatório Técnico da NetApp 4375: NetApp MetroCluster for ONTAP 9.3"	• Uma visão geral técnica da configuração e operação do MetroCluster. • Práticas recomendadas para a configuração do MetroCluster.
"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Instalação e configuração IP do MetroCluster"	• Arquitetura IP do MetroCluster • Cabeamento da configuração IP do MetroCluster • Configurando o MetroCluster no ONTAP

"Mantenha os componentes do MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster • Procedimentos de substituição ou atualização de hardware e atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração de MetroCluster elástica ou conetada à malha • Remoção automática de uma gaveta de disco em uma configuração de MetroCluster elástica ou conetada à malha • Substituição de hardware em um local de desastre em uma configuração de MetroCluster alongada ou conetada à malha • Expansão de uma configuração de MetroCluster Stretch ou conectada à malha de dois nós para uma configuração de MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster alongada ou conectada à malha de quatro nós para uma configuração de MetroCluster de oito nós.
Documentação do Active IQ Unified Manager "Documentação do NetApp: Guias de produto e recursos"	• Monitoramento da configuração e do desempenho do MetroCluster
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster

Entenda a proteção de dados e a recuperação de desastres da MetroCluster

Compreender a proteção de dados e a recuperação de desastres da MetroCluster

É útil entender como o MetroCluster protege os dados e fornece recuperação transparente contra falhas para que você possa gerenciar suas atividades de switchover e comutação de forma fácil e eficiente.

O MetroCluster usa o espelhamento para proteger os dados em um cluster. Ele fornece recuperação de desastres por meio de um único comando MetroCluster que ativa um secundário no site de sobreviventes para atender aos dados espelhados originalmente de um local principal afetado por desastre.

Como as configurações do MetroCluster de oito e quatro nós fornecem failover e switchover locais

As configurações de MetroCluster de oito e quatro nós protegem os dados em nível local e no nível do cluster. Se você estiver configurando uma configuração do MetroCluster, precisará saber como as configurações do MetroCluster protegem seus dados.

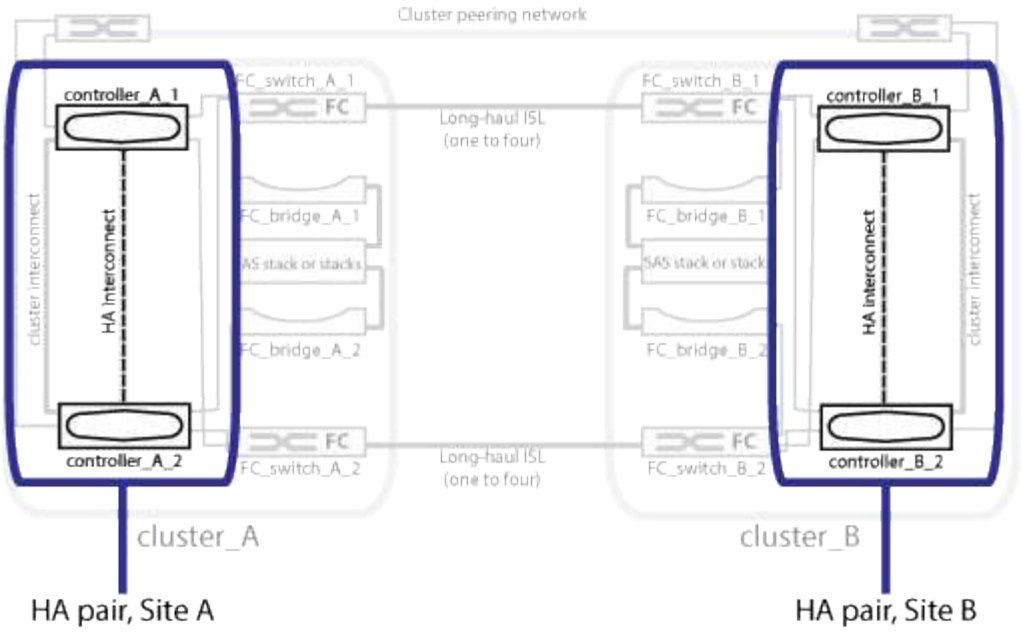
As configurações do MetroCluster protegem os dados usando dois clusters espelhados separados fisicamente. Cada cluster espelha de forma síncrona a configuração de máquina virtual de storage e dados (SVM) do outro. Quando um desastre ocorre em um local, o administrador pode ativar o SVM espelhado e começar a fornecer os dados espelhados do local que sobreviveu. Além disso, os nós em cada cluster são configurados como um par de HA, fornecendo um nível de failover local.

Como a proteção de dados de HA local funciona em uma configuração do MetroCluster

Você precisa entender como os pares de HA funcionam na configuração do MetroCluster.

Os dois clusters na rede com peering fornecem recuperação de desastres bidirecional, onde cada cluster pode ser a origem e o backup do outro cluster. Cada cluster inclui dois nós, que são configurados como um par de HA. Em caso de falha ou manutenção necessária na configuração de um único nó, o failover de storage pode transferir as operações desse nó para seu parceiro de HA local.

A ilustração a seguir mostra uma configuração MetroCluster FC. A funcionalidade de HA é a mesma nas configurações IP do MetroCluster, exceto que a interconexão de HA é fornecida pelos switches do cluster.



Informações relacionadas

"Configuração de alta disponibilidade"

Como as configurações do MetroCluster fornecem replicação de dados e configuração

As configurações do MetroCluster usam vários recursos do ONTAP para fornecer replicação síncrona de dados e configuração entre os dois locais do MetroCluster.

Proteção de configuração com o serviço de replicação de configuração

O CRS (serviço de replicação de configuração) do ONTAP protege a configuração do MetroCluster replicando automaticamente as informações para o parceiro DR.

O CRS replica de forma síncrona a configuração do nó local para o parceiro de DR no cluster de parceiros. Essa replicação é realizada pela rede de peering de cluster.

As informações replicadas incluem a configuração de cluster e a configuração SVM.

Replicação de SVMs durante as operações do MetroCluster

O CRS (serviço de replicação de configuração) do ONTAP fornece configuração redundante de servidor de dados e espelhamento de volumes de dados pertencentes ao SVM. Se ocorrer um switchover, a SVM de origem será reduzida e o SVM de destino, localizado no cluster sobrevivente, ficará ativo.

> Os SVMs de destino na configuração do MetroCluster têm o sufixo "'-mc" automaticamente anexado ao seu nome para ajudar a identificá-los. Uma configuração MetroCluster anexa o sufixo "'-mc" ao nome dos SVMs de destino, se o nome da SVM contiver um ponto, o sufixo "'-mc" é aplicado antes do primeiro período. Por exemplo, se o nome do SVM for SVM.DNS.NAME, o sufixo "'-mc" será anexado como SVM-MC.DNS.NAME.

O exemplo a seguir mostra os SVMs para uma configuração do MetroCluster, em que "'SVM_cluster_A'" é um SVM no local de origem e "'SVM_cluster_A-mc'" é um agregado de destino de sincronização no local de recuperação de desastres.

- SVM_cluster_A serve dados no cluster A..

  Ele é uma SVM de origem sincronizada que representa a configuração (LIFs, protocolos e serviços) e os dados em volumes pertencentes ao SVM. A configuração e os dados são replicados para SVM_cluster_A-mc, um SVM de destino de sincronização localizado no cluster B.

- SVM_cluster_B serve dados no cluster B..

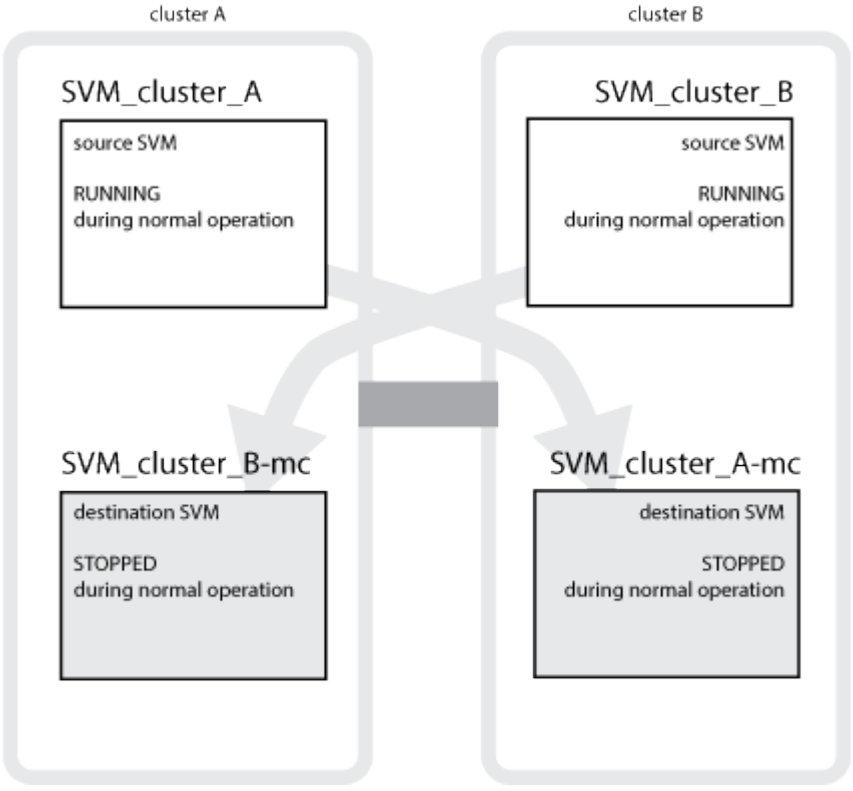
  É um SVM de origem sincronizada que representa a configuração e os dados do SVM_cluster_B-mc localizado no cluster A..

- SVM_cluster_B-mc é um SVM de destino de sincronização que é interrompido durante a operação normal e saudável da configuração do MetroCluster.

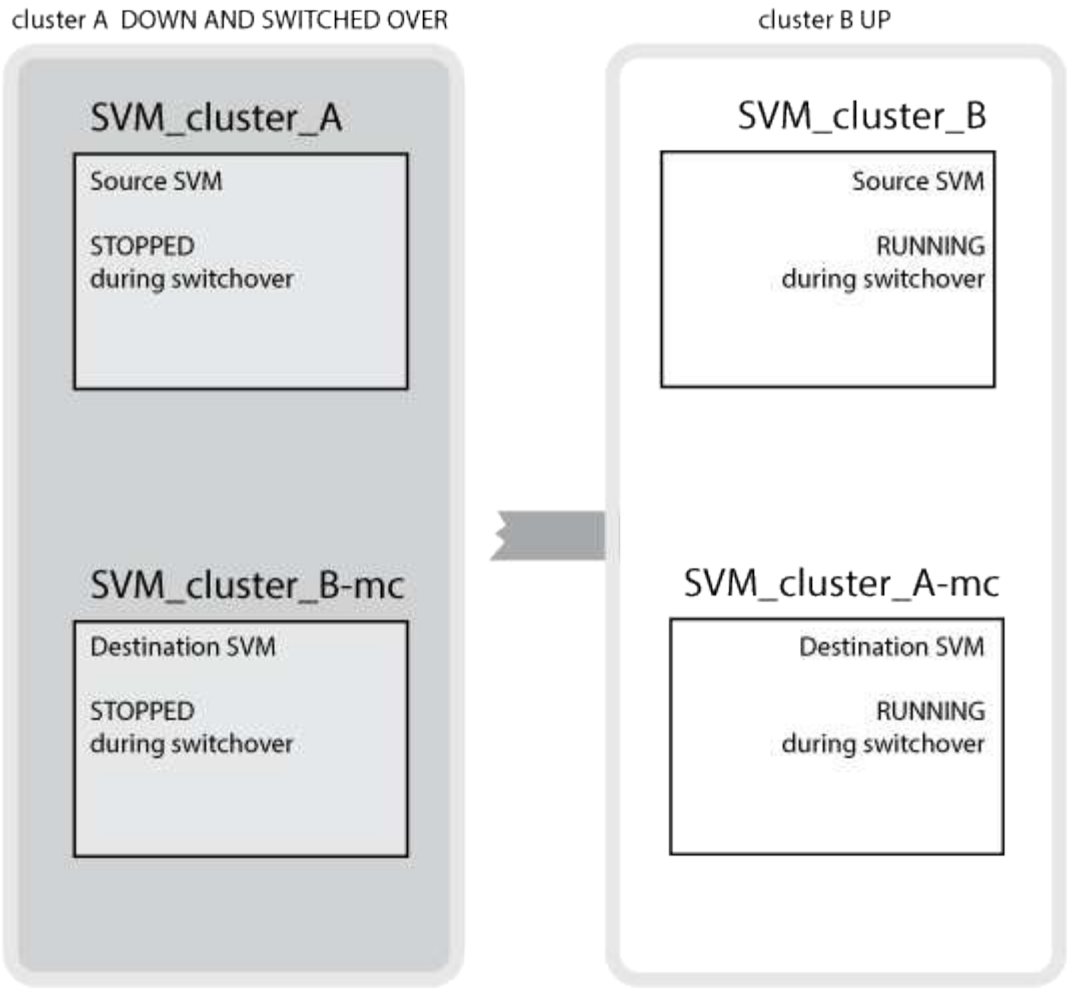
  Em um switchover bem-sucedido do cluster B para o cluster A, SVM_cluster_B é interrompido e SVM_cluster_B-mc é ativado e começa a fornecer dados do cluster A.

- SVM_cluster_A-mc é um SVM de destino de sincronização que é interrompido durante a operação normal e saudável da configuração do MetroCluster.

  Em um switchover bem-sucedido do cluster A para o cluster B, o SVM_cluster_A é interrompido e o SVM_cluster_A-mc é ativado e começa a fornecer dados do cluster B.



Se ocorrer um switchover, o Plex remoto no cluster sobrevivente fica on-line e o SVM secundário começa a fornecer os dados.



A disponibilidade de plexes remotos após o switchover depende do tipo de configuração do MetroCluster:

- Para configurações MetroCluster FC, após o switchover, os plexos locais e remotos permanecem on-line se o storage no local de desastre estiver acessível por meio de ISLs.

  Se os ISLs tiverem falhado e o storage do local de desastre não estiver disponível, o SVM de destino de sincronização começará a fornecer dados do local que sobreviveu.

- Para configurações IP do MetroCluster, a disponibilidade dos plexes remotos depende da versão do ONTAP:
  - A partir do ONTAP 9.5, os plexos locais e remotos permanecem on-line se os nós do local de desastre permanecerem inicializados.
  - Antes do ONTAP 9.5, o armazenamento está disponível apenas a partir de Plex local no local sobrevivente.

    O SVM de sincronização de destino começa a fornecer dados do local que sobreviveu.

Informações relacionadas

"Administração do sistema"

Como as configurações do MetroCluster usam o SyncMirror para fornecer redundância de dados

Agregados espelhados que usam a funcionalidade SyncMirror fornecem redundância de dados e contêm os volumes de propriedade da máquina virtual de storage de origem e destino (SVM). Os dados são replicados

em pools de discos no cluster de parceiros. Agregados não espelhados também são suportados.

A tabela a seguir mostra o estado (on-line ou off-line) de um agregado sem espelhamento após um switchover:

Tipo de comutação	Estado de configuração do MetroCluster FC	Estado de configuração IP do MetroCluster
Switchover negociado (NSO)	Online	Offline (Nota 1)
Switchover não planejado automático (AUSO)	Online	Offline (Nota 1)
Switchover não planejado (USO)	• Se o armazenamento não estiver disponível: Offline • Se o armazenamento estiver disponível: Online	Offline (Nota 1)

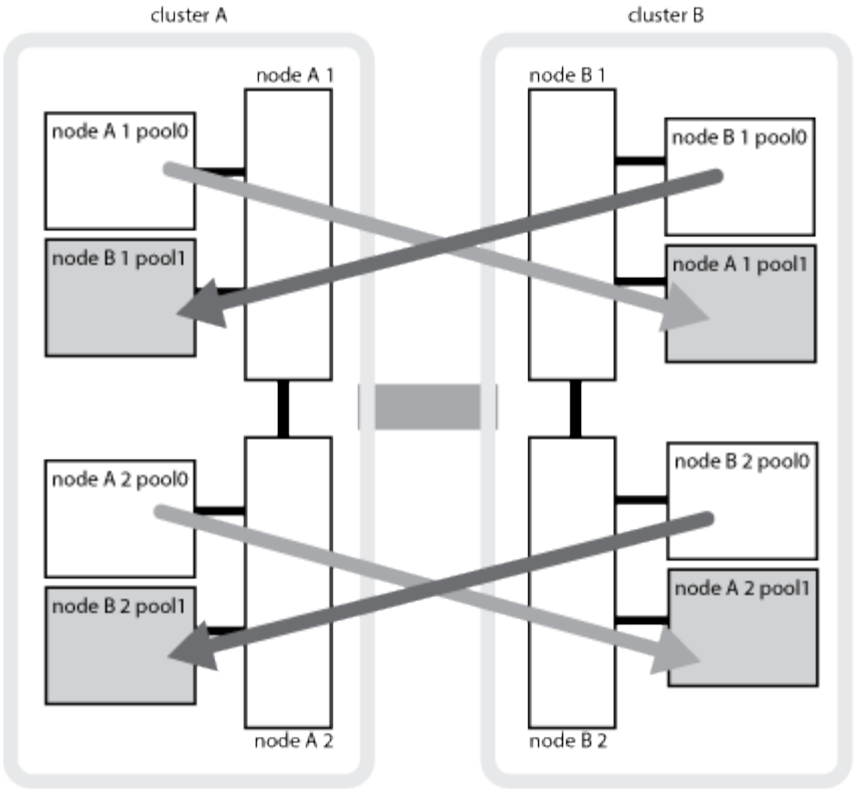
Nota 1: Nas configurações IP do MetroCluster, após a conclusão do switchover, você pode colocar manualmente os agregados sem espelhamento on-line.

Saiba mais Diferenças no switchover entre as configurações MetroCluster FC e IPsobre o .

Após um switchover, se o agregado sem espelhamento estiver no nó do parceiro de DR e houver uma falha no enlace entre switches (ISL), esse nó local pode falhar.

A ilustração a seguir mostra como os pools de discos são espelhados entre os clusters de parceiros. Os dados em plexes locais (em pool0) são replicados para plexes remotos (em pool1).

Se agregados híbridos forem usados, a degradação do desempenho pode ocorrer depois que um Plex SyncMirror falhou devido ao preenchimento da camada de disco de estado sólido (SSD).



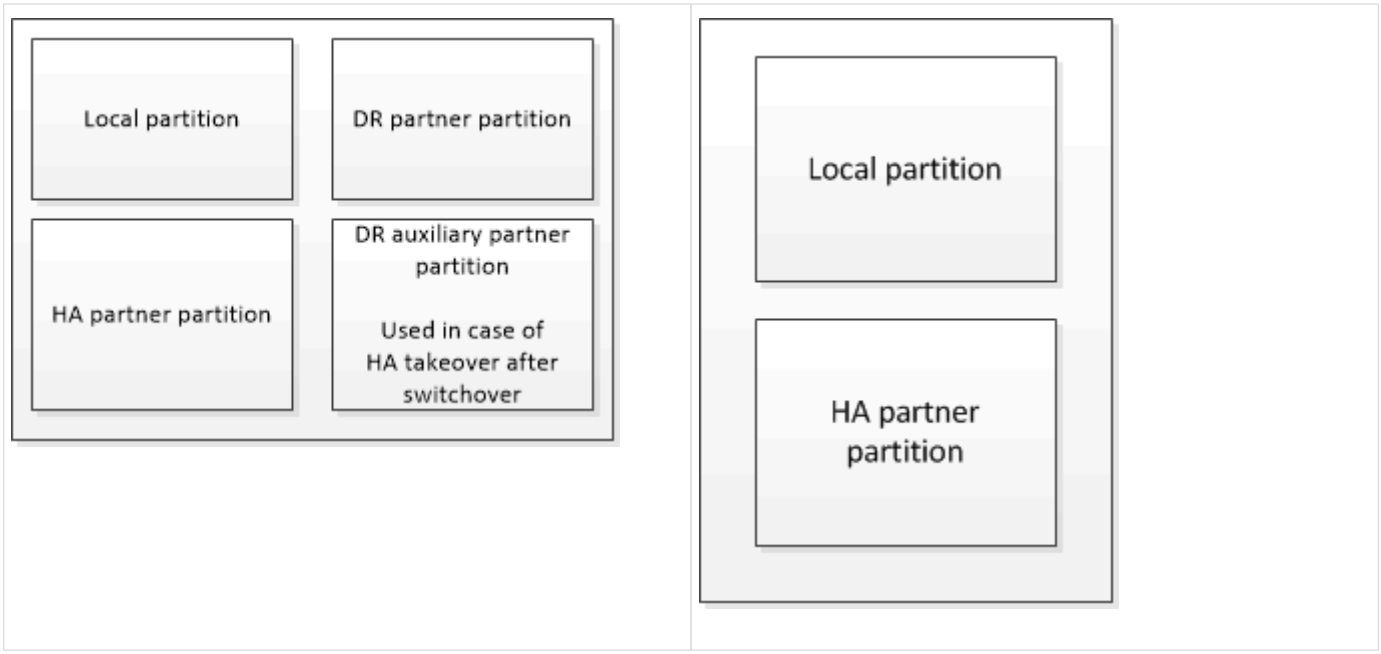
Como o espelhamento de cache NVRAM ou NVMEM e o espelhamento dinâmico funcionam nas configurações do MetroCluster

A memória não volátil (NVRAM ou NVMEM, dependendo do modelo da plataforma) nos controladores de storage é espelhada localmente para um parceiro de HA local e remotamente para um parceiro de recuperação de desastres (DR) remoto no local do parceiro. No caso de um failover local ou switchover, essa configuração permite que os dados no cache não volátil sejam preservados.

Em um par de HA que não faz parte de uma configuração do MetroCluster, cada controlador de storage mantém duas partições de cache não volátil: Uma para si e outra para seu parceiro de HA.

Em uma configuração de MetroCluster de quatro nós, o cache não volátil de cada controlador de storage é dividido em quatro partições. Em uma configuração de MetroCluster de dois nós, a partição do parceiro de HA e a partição auxiliar de DR não são usadas, porque os controladores de storage não são configurados como um par de HA.

Caches não voláteis para um controlador de storage	
Em uma configuração MetroCluster	Em um par de HA que não seja da MetroCluster



Os caches não voláteis armazenam o seguinte conteúdo:

- A partição local mantém os dados que o controlador de armazenamento ainda não gravou no disco.
- A partição do parceiro HA contém uma cópia do cache local do parceiro HA do controlador de armazenamento.

  Em uma configuração de MetroCluster de dois nós, não há nenhuma partição de parceiro de HA porque os controladores de storage não estão configurados como um par de HA.

- A partição do parceiro de DR contém uma cópia do cache local do parceiro de DR do controlador de armazenamento.

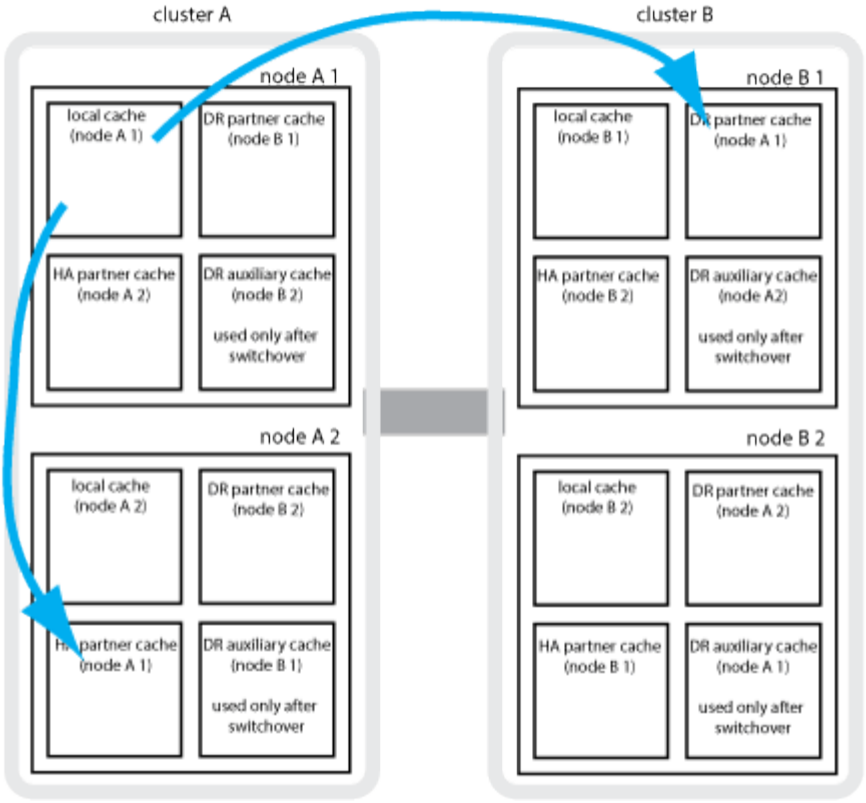
  O parceiro de DR é um nó no cluster de parceiros que é emparelhado com o nó local.

- A partição do parceiro auxiliar DR contém uma cópia do cache local do parceiro auxiliar DR do controlador de armazenamento.

  O parceiro auxiliar de DR é o parceiro de HA do parceiro de DR do nó local. Esse cache é necessário se houver um takeover de HA (quando a configuração estiver em operação normal ou após um switchover de MetroCluster).

  Em uma configuração de MetroCluster de dois nós, não há nenhuma partição auxiliar de DR porque os controladores de storage não estão configurados como um par de HA.

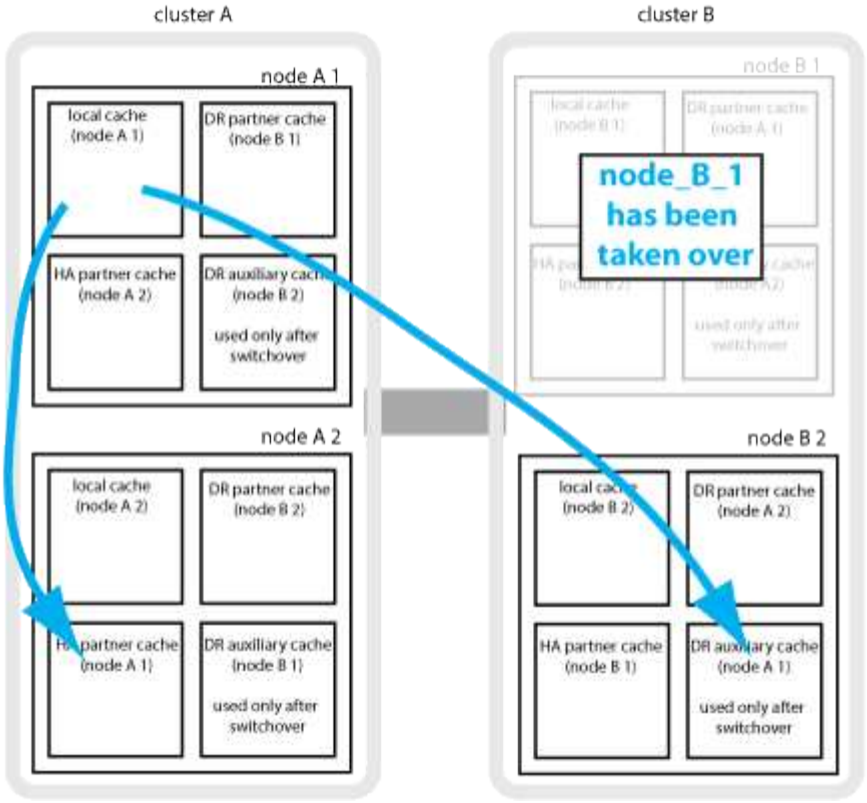
Por exemplo, o cache local de um nó (node_A_1) é espelhado tanto localmente quanto remotamente nos sites da MetroCluster. A ilustração a seguir mostra que o cache local de node_A_1 é espelhado para o parceiro de HA (node_A_2) e o parceiro de DR (node_B_1):



Espelhamento dinâmico em caso de takeover de HA local

Se um takeover de HA local ocorrer em uma configuração de MetroCluster de quatro nós, o nó assumido não poderá mais funcionar como um espelhamento para seu parceiro de DR. Para permitir que o espelhamento de DR continue, o espelhamento muda automaticamente para o parceiro auxiliar de DR. Depois de um giveback bem-sucedido, o espelhamento retorna automaticamente ao parceiro de DR.

Por exemplo, node_B_1 falha e é assumido por node_B_2. O cache local de node_A_1 não pode mais ser espelhado para node_B_1. O espelhamento muda para o parceiro auxiliar de DR, node_B_2.



Tipos de desastres e métodos de recuperação

Você precisa estar familiarizado com diferentes tipos de falhas e desastres para usar a configuração do MetroCluster para responder adequadamente.

- Falha de nó único

  Um único componente no par de HA local falha.

  Em uma configuração de MetroCluster de quatro nós, essa falha pode levar a um takeover automático ou negociado do nó afetado, dependendo do componente que falhou. A recuperação de dados é descrita em "Gerenciamento de pares de alta disponibilidade" .

  Em uma configuração de MetroCluster de dois nós, essa falha leva a um switchover não planejado automático (AUSO).

- Falha no controlador em todo o local

  Todos os módulos do controlador falham em um local devido à perda de energia, substituição de equipamentos ou desastre. Normalmente, as configurações do MetroCluster não conseguem diferenciar entre falhas e desastres. No entanto, o software Witness, como o software tiebreaker da MetroCluster, pode diferenciar entre eles. Uma condição de falha do controlador em todo o local pode levar a um switchover automático se os links e switches do Inter-Switch Link (ISL) estiverem ativos e o armazenamento estiver acessível.

  "Gerenciamento de pares de alta disponibilidade" tem mais informações sobre como recuperar de falhas de controladora em todo o local que não incluem falhas de controladora, bem como falhas que incluem um ou mais controladores.

- Falha ISL

Os links entre os sites falham. A configuração do MetroCluster não toma nenhuma ação. Cada nó continua fornecendo dados normalmente, mas os espelhos não são gravados nos respetivos locais de recuperação de desastres, pois o acesso a eles é perdido.

- Várias falhas sequenciais

  Vários componentes falham em uma sequência. Por exemplo, um módulo de controladora, uma malha de switch e uma gaveta falham em uma sequência e resultam em um failover de storage, redundância de malha e proteção sequencial do SyncMirror contra tempo de inatividade e perda de dados.

A tabela a seguir mostra os tipos de falha e o mecanismo de recuperação de desastres (DR) correspondente e o método de recuperação:

> O AUSO (switchover não planejado automático) não é suportado em configurações IP do MetroCluster.

Tipo de falha	Mecanismo DR		Resumo do método de recuperação	
	Configuração de quatro nós	Configuração de dois nós	Configuração de quatro nós	Configuração de dois nós
Falha de nó único	Failover local de HA	AUSO	Não é necessário se o failover automático e a giveback estiverem ativados.	Depois que o nó é restaurado, a recuperação manual e o switchback usando os `metrocluster heal -phase aggregates` comandos , `metrocluster heal -phase root-aggregates`, e `metrocluster switchback` são necessários. NOTA: Os `metrocluster heal` comandos não são necessários nas configurações IP do MetroCluster executando o ONTAP 9.5 ou posterior.

Falha do local	Switchover do MetroCluster		Depois que o nó é restaurado, a recuperação manual e o switchback usando os `metrocluster healing` comandos e `metrocluster switchback` são necessários. Os `metrocluster heal` comandos não são necessários nas configurações IP do MetroCluster que executam o ONTAP 9.5.
Falha no controlador em todo o local	AUSO apenas se o armazenamento no local de desastre estiver acessível.	AUSO (mesmo que falha de nó único)	
Várias falhas sequenciais	Failover de HA local seguido de switchover forçado pelo MetroCluster usando o comando MetroCluster switchover - forçado no desastre. Nota: Dependendo do componente que falhou, pode não ser necessário um switchover forçado.	MetroCluster comutação forçada usando o `metrocluster switchover -forced-on -disaster` comando.	
Falha ISL	Sem switchover do MetroCluster; os dois clusters servem seus dados de forma independente		Não é necessário para este tipo de falha. Depois de restaurar a conetividade, o armazenamento ressincroniza automaticamente.

Como uma configuração de MetroCluster de oito ou quatro nós fornece operações ininterruptas

No caso de um problema limitado a um único nó, um failover e giveback no par de HA local fornecem operações ininterruptas contínuas. Nesse caso, a configuração do MetroCluster não requer um switchover para o local remoto.

Como a configuração do MetroCluster de oito ou quatro nós consiste em um ou mais par de HA em cada local, cada local pode resistir a falhas locais e executar operações ininterruptas sem exigir um switchover para o local do parceiro. A operação do par de HA é a mesma que os pares de HA em configurações que não sejam da MetroCluster.

Para configurações de MetroCluster de quatro e oito nós, falhas nos nós devido a pânico ou perda de energia podem causar um switchover automático.

"Gerenciamento de pares de alta disponibilidade"

Se uma segunda falha ocorrer após um failover local, o evento de switchover do MetroCluster fornecerá operações ininterruptas contínuas. Da mesma forma, após uma operação de switchover, no caso de uma segunda falha em um dos nós sobreviventes, um evento de failover local fornece operações ininterruptas contínuas. Nesse caso, o nó único sobrevivente serve dados para os outros três nós no grupo de DR.

Comutação e switchback durante a transição do MetroCluster

A transição de FC para IP do MetroCluster envolve a adição de nós IP e switches IP do MetroCluster a uma configuração de FC do MetroCluster existente e a desativação dos nós FC do MetroCluster. Dependendo da etapa do processo de transição, as operações de comutação, recuperação e switchback do MetroCluster usam fluxos de trabalho diferentes.

```
http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-mcc-upgrade/GUID-1870FDC4-1774-4604-86A7-5C979C297ADA.html["Operações de switchover, recuperação e switchback durante a transição"^]Consulte .
```

Consequências do failover local após o switchover

Se ocorrer um switchover do MetroCluster e surgir um problema no local que sobreviveu, um failover local pode fornecer operações contínuas e sem interrupções. No entanto, o sistema está em risco porque não está mais em uma configuração redundante.

Se um failover local ocorrer após a ocorrência de um switchover, uma única controladora fornecerá dados para todos os sistemas de storage na configuração MetroCluster, levando a possíveis problemas de recursos, e estará vulnerável a falhas adicionais.

Como uma configuração de MetroCluster de dois nós fornece operações ininterruptas

Se um dos dois locais apresentar algum problema devido a pânico, o switchover do MetroCluster fornece uma operação contínua sem interrupções. Se a perda de energia afetar o nó e o storage, o switchover não será automático e haverá interrupção até que o `metrocluster switchover` comando seja emitido.

Como todo o storage é espelhado, uma operação de switchover pode ser usada para fornecer resiliência sem interrupções no caso de uma falha no local semelhante à encontrada em um failover de storage em um par de HA para uma falha de nó.

Para configurações de dois nós, os mesmos eventos que acionam um failover automático de storage em um par de HA acionam um switchover automático não planejado (AUSO). Isso significa que uma configuração de MetroCluster de dois nós tem o mesmo nível de proteção que um par de HA.

Informações relacionadas

"Switchover automático não planejado em configurações de MetroCluster FC"

Visão geral do processo de transição

A operação de switchover do MetroCluster permite a retomada imediata dos serviços após um desastre, movendo o storage e o acesso do cliente do cluster de origem para o local remoto. Você precisa estar ciente das mudanças a esperar e quais ações você precisa executar se um switchover ocorrer.

Durante uma operação de comutação, o sistema executa as seguintes ações:

- A propriedade dos discos que pertencem ao local de desastre é alterada para o parceiro de recuperação de desastre (DR).

  Isso é semelhante ao caso de um failover local em um par de alta disponibilidade (HA), no qual a propriedade dos discos pertencentes ao parceiro inativo é alterada para o parceiro íntegro.

- Os plexo sobreviventes que estão localizados no local sobrevivente, mas pertencem aos nós no cluster de desastres, são colocados on-line no cluster no local sobrevivente.
- A máquina virtual de storage de origem síncrona (SVM) que pertence ao local do desastre é reduzida apenas durante um switchover negociado.

Isto é aplicável apenas a uma mudança negociada.

- É apresentada a SVM de sincronização de destino pertencente ao local do desastre.

Ao serem trocados, os agregados raiz do parceiro de DR não são disponibilizados online.

O `metrocluster switchover` comando alterna entre os nós em todos os grupos de DR na configuração MetroCluster. Por exemplo, em uma configuração de MetroCluster de oito nós, ele alterna entre os nós em ambos os grupos de DR.

Se você estiver trocando apenas serviços para o local remoto, você deve executar um switchover negociado sem cercar o local. Se o storage ou o equipamento não forem confiáveis, você deve cercar o local de desastre e, em seguida, executar um switchover não planejado. O cerco impede reconstruções RAID quando os discos são ligados de forma escalonada.

Este procedimento só deve ser usado se o outro site for estável e não se pretende ficar offline.

Disponibilidade de comandos durante o switchover

A tabela a seguir mostra a disponibilidade de comandos durante o switchover:

Comando	Disponibilidade
`storage aggregate create`	Você pode criar um agregado: • Se for propriedade de um nó que faz parte do cluster sobrevivente Não é possível criar um agregado: • Para um nó no local do desastre • Para um nó que faz parte do cluster sobrevivente
`storage aggregate delete`	Você pode excluir um agregado de dados.
`storage aggregate mirror`	Você pode criar um Plex para um agregado não espelhado.
`storage aggregate plex delete`	Você pode excluir um Plex para um agregado espelhado.
`vserver create`	Você pode criar um SVM: • Se seu volume raiz reside em um agregado de dados de propriedade do cluster sobrevivente Não é possível criar um SVM: • Se o volume raiz dele residir em um agregado de dados de propriedade do cluster do local de desastre

`vserver delete`	Você pode excluir SVMs de origem e destino de sincronização.
`network interface create -lif`	Você pode criar um data SVM LIF para SVMs de sincronização e destino.
`network interface delete -lif`	Você pode excluir um data SVM LIF para SVMs de origem e destino de sincronização.
`volume create`	Você pode criar um volume para SVMs de origem sincronizada e destino de sincronização. • Para uma SVM de origem sincronizada, o volume deve residir em um agregado de dados pertencente ao cluster sobrevivente • Para uma SVM de destino sincronizado, o volume precisa residir em um agregado de dados de propriedade do cluster do local de desastre
`volume delete`	Você pode excluir um volume para SVMs de origem e destino de sincronização.
`volume move`	Você pode mover um volume para SVMs de origem sincronizada e destino de sincronização. • Para uma SVM de origem sincronizada, o cluster sobrevivente deve possuir o agregado de destino • Para uma SVM de destino sincronizado, o cluster do local de desastre precisa ser proprietário do agregado de destino
`snapmirror break`	Você pode quebrar uma relação do SnapMirror entre um ponto de extremidade de origem e destino de um espelho de proteção de dados.

Diferenças no switchover entre as configurações MetroCluster FC e IP

Nas configurações IP do MetroCluster, como os discos remotos são acessados por meio dos nós de parceiros de DR remotos que atuam como destinos iSCSI, os discos remotos não são acessíveis quando os nós remotos são derrubados em uma operação de switchover. Isso resulta em diferenças com as configurações do MetroCluster FC:

- Agregados espelhados que são de propriedade do cluster local tornam-se degradados.
- Agregados espelhados que foram comutados pelo cluster remoto se degradam.

Quando agregados sem espelhamento são suportados em uma configuração MetroCluster IP, os agregados sem espelhamento que não são comutados pelo cluster remoto não são acessíveis.

Alterações na propriedade do disco durante o takeover de HA e o switchover do MetroCluster em uma configuração de MetroCluster de quatro nós

A propriedade dos discos muda temporariamente automaticamente durante as operações de alta disponibilidade e MetroCluster. É útil saber como o sistema rastreia qual nó possui quais discos.

No ONTAP, o ID de sistema exclusivo de um módulo de controlador (obtido a partir da placa NVRAM ou da placa NVMEM de um nó) é usado para identificar qual nó possui um disco específico. Dependendo do estado de HA ou DR do sistema, a propriedade do disco pode mudar temporariamente. Se a propriedade mudar devido a uma tomada de controle de HA ou um switchover de DR, o sistema Registra qual nó é o proprietário original (chamado de "casa") do disco, de modo que ele possa retornar a propriedade após HA giveback ou DR switchback. O sistema utiliza os seguintes campos para controlar a propriedade do disco:

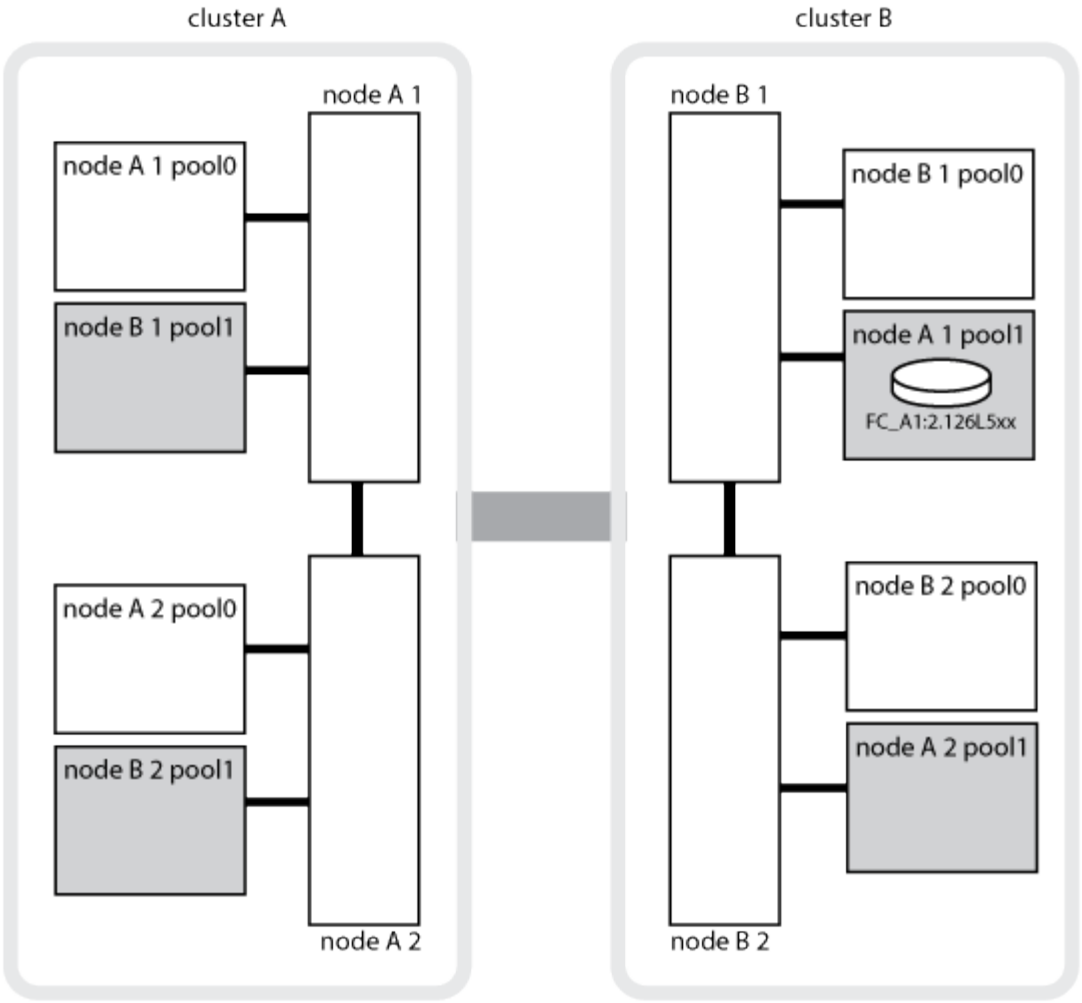
- Proprietário
- Proprietário da casa
- Proprietário do DR Home

Na configuração do MetroCluster, no caso de um switchover, um nó pode se apropriar de um agregado de propriedade original de nós no cluster de parceiros. Esses agregados são chamados de agregados estranhos em cluster. A caraterística distintiva de um agregado cluster-estrangeiro é que ele é um agregado não conhecido atualmente pelo cluster e, portanto, o campo proprietário do DR Home é usado para mostrar que ele é de propriedade de um nó do cluster de parceiros. Um agregado estrangeiro tradicional dentro de um par de HA é identificado pelo proprietário e os valores do proprietário do lar sendo diferentes, mas os valores do proprietário e do proprietário do lar são os mesmos para um agregado estrangeiro de cluster; assim, você pode identificar um agregado estrangeiro de cluster pelo valor do proprietário do lar DR.

À medida que o estado do sistema muda, os valores dos campos mudam, como mostrado na tabela a seguir:

Campo	Valor durante…			
	Funcionamento normal	Takeover local de HA	Switchover do MetroCluster	Aquisição durante o switchover
Proprietário	ID do nó que tem acesso ao disco.	ID do parceiro de HA, que tem temporariamente acesso ao disco.	ID do parceiro DR, que tem acesso temporário ao disco.	ID do parceiro auxiliar DR, que tem temporariamente acesso ao disco.
Proprietário da casa	ID do proprietário original do disco dentro do par de HA.	ID do proprietário original do disco dentro do par de HA.	ID do parceiro DR, que é o proprietário do lar no par de HA durante o switchover.	ID do parceiro DR, que é o proprietário do lar no par de HA durante o switchover.
Proprietário do DR Home	Vazio	Vazio	ID do proprietário original do disco dentro da configuração do MetroCluster.	ID do proprietário original do disco dentro da configuração do MetroCluster.

A ilustração e tabela a seguir fornecem um exemplo de como a propriedade muda, para um disco no disco pool1 do node_A_1, localizado fisicamente no cluster_B.



Estado de MetroCluster	Proprietário	Proprietário da casa	Proprietário do DR Home	Notas
Normal com todos os nós totalmente operacionais.	node_A_1	node_A_1	não aplicável	
Takeover de HA local, node_A_2 assumiu os discos pertencentes ao seu parceiro de HA node_A_1.	node_A_2	node_A_1	não aplicável	

O switchover de DR, node_B_1 assumiu o controle de discos pertencem a seu parceiro de DR, node_A_1.	node_B_1	node_B_1	node_A_1	O ID do nó inicial original é movido para o campo proprietário do DR Home. Após o switchback agregado ou a recuperação, a propriedade volta para node_A_1.
No switchover de DR e no controle local de HA (falha dupla), o node_B_2 assumiu os discos pertencentes ao seu nó de HA_B_1.	node_B_2	node_B_1	node_A_1	Após a giveback, a propriedade volta para node_B_1. Após o switchback ou a recuperação, a propriedade volta para node_A_1.
Após o switchback de recuperação de desastres e de HA, todos os nós estão totalmente operacionais.	node_A_1	node_A_1	não aplicável	

Considerações ao usar agregados sem espelhamento

Se a sua configuração incluir agregados sem espelhamento, você precisa estar ciente de possíveis problemas de acesso após as operações de switchover.

Considerações para agregados sem espelhamento ao fazer manutenção que requer desligamento de energia

Se você estiver executando o switchover negociado por motivos de manutenção que exigem desligamento de energia em todo o local, primeiro deverá ficar offline manualmente todos os agregados sem espelhamento pertencentes ao local de desastre.

Se você não fizer isso, os nós no local sobrevivente podem descer devido a panics de vários discos. Isso pode ocorrer se agregados sem espelhamento com comutação ficarem off-line ou estiverem ausentes devido à perda de conetividade ao storage no local de desastre devido ao desligamento de energia ou à perda de ISLs.

Considerações para agregados sem espelhamento e namespaces hierárquicos

Se você estiver usando namespaces hierárquicos, você deve configurar o caminho de junção para que todos os volumes nesse caminho estejam apenas em agregados espelhados ou apenas em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados no caminho de junção pode impedir o acesso aos agregados sem espelhamento após a operação de comutação.

Considerações para agregados sem espelhamento e volumes de metadados CRS e volumes raiz de dados SVM

O volume de metadados do serviço de replicação de configuração (CRS) e os volumes raiz de dados do SVM devem estar em um agregado espelhado. Não é possível mover esses volumes para agregado sem

espelhamento. Se eles estiverem em operações de comutação e switchback negociadas sem espelhamento, serão vetadas. O `metrocluster check` comando fornece um aviso se for esse o caso.

Considerações para agregados sem espelhamento e SVMs

Os SVMs devem ser configurados somente em agregados espelhados ou somente em agregados sem espelhamento. Configurar uma combinação de agregados sem espelhamento e espelhados pode resultar em uma operação de switchover que excede 120 segundos e resultar em uma interrupção de dados se os agregados sem espelhamento não ficarem online.

Considerações para agregados sem espelhamento e SAN

Um LUN não deve estar localizado em um agregado sem espelhamento. Configurar um LUN em um agregado sem espelhamento pode resultar em uma operação de switchover que excede 120 segundos e uma interrupção de dados.

Switchover automático não planejado em configurações de MetroCluster FC

Em configurações de FC do MetroCluster, certos cenários podem acionar um switchover não planejado automático (AUSO) no caso de uma falha do controlador em todo o local para fornecer operações ininterruptas. O AUSO pode ser desativado se desejado.

O switchover não planejado automático não é suportado nas configurações IP do MetroCluster.

Em uma configuração MetroCluster FC, um AUSO pode ser acionado se todos os nós de um local falharem devido aos seguintes motivos:

- Desligar
- Perda de energia
- Pânico

Em uma configuração MetroCluster FC de oito nós, você pode definir uma opção para acionar um AUSO se ambos os nós em um par de HA falharem.

Como não há failover de HA local disponível em uma configuração de MetroCluster de dois nós, o sistema executa um AUSO para fornecer operação contínua após uma falha da controladora. Esse recurso é semelhante ao recurso de takeover de HA em um par de HA. Em uma configuração de MetroCluster de dois nós, um AUSO pode ser acionado nos seguintes cenários:

- Desativação do nó
- Perda de energia do nó
- Pânico do nó
- Reinicialização do nó

Se ocorrer um AUSO, a propriedade de disco para os discos pool0 e pool1 do nó prejudicado será alterada para o parceiro de recuperação de desastres (DR). Essa mudança de propriedade impede que os agregados entrem em um estado degradado após o switchover.

Após o switchover automático, você precisa prosseguir manualmente as operações de recuperação e switchback para retornar o controlador à operação normal.

AUSO assistido por hardware em configurações de MetroCluster de dois nós

Em uma configuração de MetroCluster de dois nós, o processador de serviço (SP) do módulo do controlador monitora a configuração. Em alguns cenários, o SP pode detetar uma falha mais rápida do que o software ONTAP. Neste caso, o SP aciona o AUSO. Esta funcionalidade é ativada automaticamente.

O SP envia e recebe tráfego SNMP de e para seu parceiro de DR para monitorar sua integridade.

Alteração da configuração AUSO nas configurações do MetroCluster FC

O AUSO está definido como "auso-on-cluster-disaster" por padrão. Seu status pode ser visto no `metrocluster show` comando.

> A configuração AUSO não se aplica às configurações IP do MetroCluster.

Você pode desativar o AUSO com o `metrocluster modify -auto-switchover-failure-domain auto-disabled` comando. Este comando impede o acionamento do AUSO na falha do controlador de todo o local de DR. Ele deve ser executado em ambos os sites se você quiser desativar o AUSO em ambos os sites.

AUSO pode ser reativado com o `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster` comando.

AUSO também pode ser definido como ""auso-on-dr-group-disaster". Esse comando de nível avançado aciona o AUSO no failover de HA em um local. Ele deve ser executado em ambos os sites com o `metrocluster modify -auto-switchover-failure-domain auso-on-dr-group-disaster` comando.

A definição AUSO durante o switchover

Quando o switchover ocorre, a configuração AUSO é desativada internamente porque, se um local estiver em switchover, ele não poderá alternar automaticamente.

Recuperando-se da AUSO

Para se recuperar de um AUSO, você executa os mesmos passos que para um switchover planejado.

"Realização de comutação para testes ou manutenção"

Switchover não planejado e automático assistido por mediador em configurações de IP do MetroCluster

"Saiba mais sobre como o Mediador ONTAP suporta o switchover não planejado automático em configurações IP do MetroCluster".

O que acontece durante a recuperação (configurações de MetroCluster FC)

Durante a recuperação em configurações de MetroCluster FC, a ressincronização de agregados espelhados ocorre em um processo faseado que prepara os nós no local de desastre reparado para switchback. É um evento planejado, proporcionando controle total de cada etapa para minimizar o tempo de inatividade. A recuperação é um processo de duas etapas que ocorre nos componentes do storage e do controlador.

Recuperação de agregado de dados

Depois que o problema no local de desastre for resolvido, você inicia a fase de recuperação de storage:

1. Verifica se todos os nós estão ativos e em execução no local sobrevivente.
2. Altera a propriedade de todos os discos do pool 0 no local de desastre, incluindo agregados de raiz.

Durante essa fase de recuperação, o subsistema RAID ressincroniza agregados espelhados e o subsistema WAFL replica os arquivos nvsave de agregados espelhados que tinham um pool 1 Plex com falha no momento do switchover.

Se alguns componentes de armazenamento de origem falharem, o comando reportará os erros nos níveis aplicáveis: Armazenamento, Sanown ou RAID.

Se nenhum erro for relatado, os agregados serão ressincronizados com êxito. Este processo pode às vezes levar horas para ser concluído.

"Recuperação da configuração"

Recuperação de agregado de raiz

Depois que os agregados são sincronizados, você inicia a fase de recuperação da controladora devolvendo os agregados CFO e os agregados raiz aos respetivos parceiros de DR.

"Recuperação da configuração"

O que acontece durante a recuperação (configurações MetroCluster IP)

Durante a recuperação em configurações MetroCluster IP, a ressincronização de agregados espelhados ocorre em um processo faseado que prepara os nós no local de desastre reparado para switchback. É um evento planejado, proporcionando controle total de cada etapa para minimizar o tempo de inatividade. A recuperação é um processo de duas etapas que ocorre nos componentes do storage e do controlador.

Diferenças nas configurações do MetroCluster FC

Nas configurações IP do MetroCluster, você deve inicializar os nós no cluster do local de desastre antes que a operação de recuperação seja executada.

Os nós no cluster do local de desastre devem estar em execução para que os discos iSCSI remotos possam ser acessados quando os agregados são ressincronizados.

Se os nós do local de desastre não estiverem em execução, a operação de recuperação falhará porque o nó de desastre não pode executar as alterações de propriedade do disco necessárias.

Recuperação de agregado de dados

Depois que o problema no local de desastre for resolvido, você inicia a fase de recuperação de storage:

1. Verifica se todos os nós estão ativos e em execução no local sobrevivente.
2. Altera a propriedade de todos os discos do pool 0 no local de desastre, incluindo agregados de raiz.

Durante essa fase de recuperação, o subsistema RAID ressincroniza agregados espelhados e o subsistema WAFL replica os arquivos nvsave de agregados espelhados que tinham um pool 1 Plex com falha no momento do switchover.

Se alguns componentes de armazenamento de origem falharem, o comando reportará os erros nos níveis aplicáveis: Armazenamento, Sanown ou RAID.

Se nenhum erro for relatado, os agregados serão ressincronizados com êxito. Este processo pode às vezes levar horas para ser concluído.

"Recuperação da configuração"

Recuperação de agregado de raiz

Depois que os agregados são sincronizados, você executa a fase de recuperação de agregados de raiz. Nas configurações IP do MetroCluster, essa fase confirma que os agregados foram curados.

"Recuperação da configuração"

Recuperação automática de agregados em configurações MetroCluster IP após o switchover

A partir do ONTAP 9.5, a recuperação é automatizada durante operações de switchover negociado em configurações de IP do MetroCluster. A partir do ONTAP 9.6, a recuperação automatizada após o switchover não programado é suportada. Isso remove o requisito de emitir os `metrocluster heal` comandos.

Recuperação automática após comutação negociada (começando com ONTAP 9.5)

Depois de executar um switchover negociado (um comando de switchover emitido sem a opção -forced-on -disaster true), a funcionalidade de recuperação automática simplifica as etapas necessárias para retornar o sistema à operação normal. Em sistemas com recuperação automática, o seguinte ocorre após o switchover:

- Os nós do local de desastre permanecem ativos.

  Como eles estão no estado de switchover, eles não estão fornecendo dados de seus plexos espelhados locais.

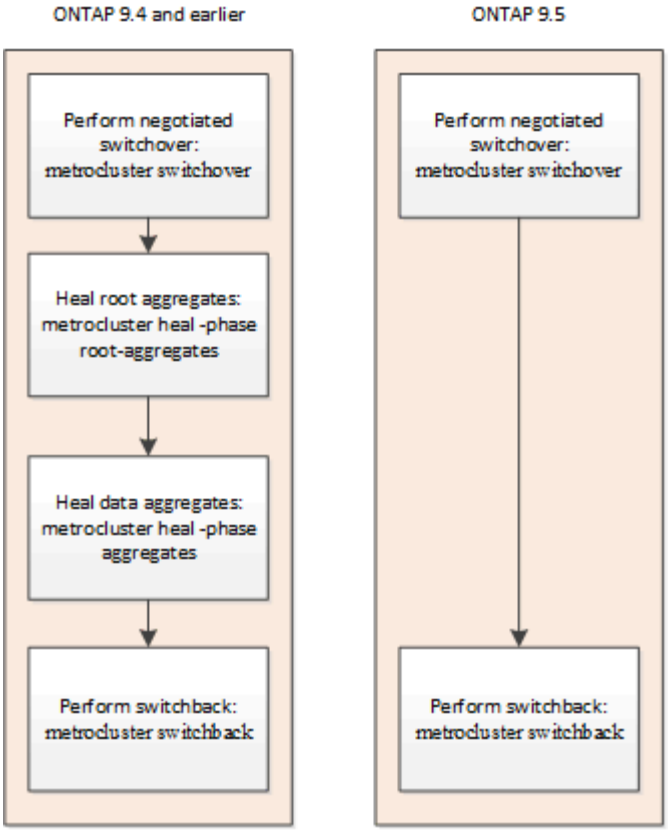
- Os nós do local de desastre são movidos para o estado "aguardando pelo switchback".

  Você pode confirmar o status dos nós do local de desastre usando o comando MetroCluster operation show.

- Você pode executar a operação de switchback sem emitir os comandos de cura.

Esse recurso se aplica às configurações IP do MetroCluster executando o ONTAP 9.5 e posterior. Isso não se aplica às configurações do MetroCluster FC.

Os comandos de recuperação manual ainda são necessários em configurações IP do MetroCluster executando o ONTAP 9.4 e anteriores.



Recuperação automática após comutação não programada (começando com ONTAP 9.6)

A recuperação automática após um switchover não programado é suportada em configurações IP do MetroCluster a partir de ONTAP 9.6. Um switchover não programado é aquele em que em você emite o `switchover` comando com a `-forced-on-disaster true` opção.

A recuperação automática após um switchover não programado não é suportada nas configurações do MetroCluster FC, e os comandos de recuperação manual ainda são necessários após o switchover não programado nas configurações do MetroCluster IP que executam o ONTAP 9.5 e anteriores.

Em sistemas que executam o ONTAP 9.6 e posterior, o seguinte ocorre após o switchover não programado:

- Dependendo da extensão do desastre, os nós do local do desastre podem estar inativos.

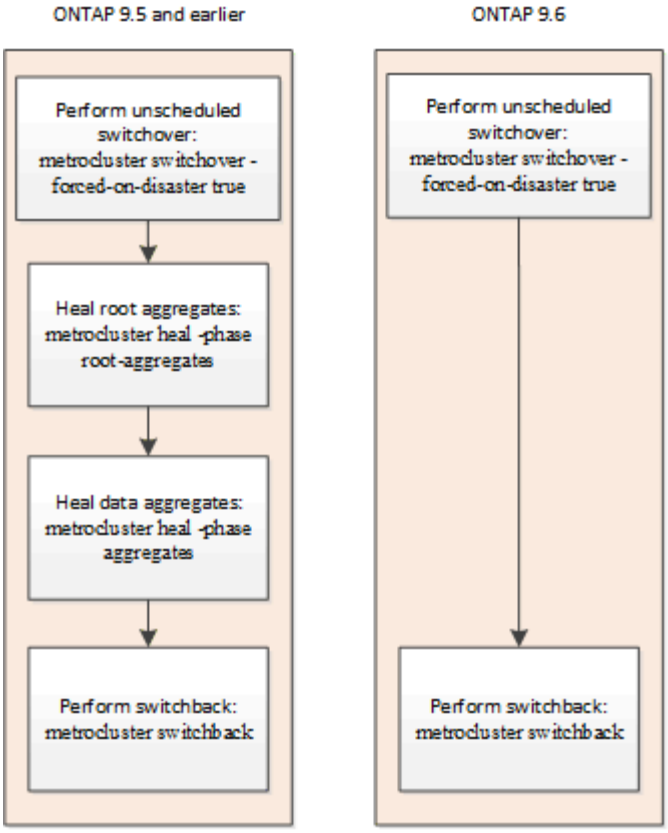
  Como eles estão no estado de comutação, eles não estão fornecendo dados de seus plexos espelhados locais, mesmo que estejam ligados.

- Se os locais de desastre estavam inativos, quando inicializados, os nós do local de desastre são movidos para o estado "aguardando pelo switchback".

  Se os locais de desastre permaneceram altos, eles são imediatamente transferidos para o estado "esperando por switchback".

- As operações de cura são realizadas automaticamente.

  Você pode confirmar o status dos nós do local de desastre e se as operações de recuperação foram bem-sucedidas usando o `metrocluster operation show` comando.



Se a recuperação automática falhar

Se a operação de recuperação automática falhar por qualquer motivo, você deve emitir os `metrocluster heal` comandos manualmente, como feito nas versões do ONTAP anteriores ao ONTAP 9.6. Você pode usar os `metrocluster operation show` comandos e `metrocluster operation history show -instance` para monitorar o status da recuperação e determinar a causa de uma falha.

Criação de SVMs para uma configuração do MetroCluster

Você pode criar SVMs para uma configuração do MetroCluster para fornecer recuperação de desastres síncrona e alta disponibilidade de dados nos clusters configurados para uma configuração do MetroCluster.

- Os dois clusters precisam estar em uma configuração MetroCluster.
- Os agregados precisam estar disponíveis e on-line em ambos os clusters.
- Se necessário, os IPspaces com os mesmos nomes devem ser criados em ambos os clusters.
- Se um dos clusters que formam a configuração do MetroCluster for reinicializado sem utilizar um switchover, então os SVMs de fonte de sincronização podem ficar online como "coberto" em vez de ""cortado"".

Quando você cria um SVM em um dos clusters em uma configuração do MetroCluster, o SVM é criado como o SVM de origem e o SVM do parceiro é criado automaticamente com o mesmo nome, mas com o sufixo "'-mc" no cluster de parceiros. Se o nome do SVM contiver um ponto, o sufixo "'-mc" é aplicado antes do primeiro período, por exemplo, SVM-MC.DNS.NAME.

Em uma configuração do MetroCluster, você pode criar 64 SVMs em um cluster. Uma configuração do MetroCluster oferece suporte a 128 SVMs.

1. Use o `vserver create` comando.

   O exemplo a seguir mostra o SVM com o subtipo "sync-source" no local e o SVM com o subtipo "sync-destination" no local do parceiro:

   ```
   cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -aggregate
   aggr1
   -rootvolume-security-style mixed
   [Job 196] Job succeeded:
   Vserver creation completed
   ```

   O SVM "'VS4'" é criado no local e o SVM "'VS4-mc'" é criado no local do parceiro.

2. Veja os SVMs recém-criados.

   - No cluster local, verifique o estado de configuração das SVMs:

     `metrocluster vserver show`

     O exemplo a seguir mostra os SVMs do parceiro e seu estado de configuração:

     ```
     cluster_A::> metrocluster vserver show

                          Partner    Configuration
     Cluster     Vserver   Vserver    State
     ---------  --------  --------- -----------------
     cluster_A   vs4       vs4-mc     healthy
     cluster_B   vs1       vs1-mc     healthy
     ```

   - Nos clusters local e de parceiros, verifique o estado dos SVMs recém-configurados:

     `vserver show command`

     O exemplo a seguir exibe os estados administrativos e operacionais dos SVMs:

```
cluster_A::> vserver show

                              Admin   Operational Root
Vserver Type  Subtype         State   State       Volume     Aggregate
------- ----- -------       ------- --------    -----------
----------
vs4     data  sync-source   running   running    vs4_root   aggr1

cluster_B::> vserver show

                                Admin   Operational  Root
Vserver Type  Subtype           State   State        Volume
Aggregate
------- ----- -------           ------  ---------    -----------
----------
vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
```

A criação de SVM pode falhar se quaisquer operações intermediárias, como criação de volume raiz, falharem e o SVM estiver no estado ""inicializando"". Você precisa excluir o SVM e recriá-lo.

Os SVMs para a configuração MetroCluster são criados com um volume raiz de 1 GB. O SVM de origem sincronizada está no estado "em execução" e o SVM de destino de sincronização está no estado "coberto".

O que acontece durante um switchback

Após a recuperação do local de desastre e a recuperação dos agregados, o processo de switchback do MetroCluster retorna o storage e o acesso do cliente do local de recuperação de desastres para o cluster doméstico.

O `metrocluster switchback` comando retorna o local principal para operação MetroCluster completa e normal. Quaisquer alterações de configuração são propagadas para os SVMs originais. A operação do servidor de dados é retornada às SVMs de origem sincronizada no local de desastre e os SVMs de destino de sincronização que estavam operando no site sobrevivente são desativados.

Se os SVMs foram excluídos no local sobrevivente enquanto a configuração do MetroCluster estava no estado de comutação, o processo de switchback faz o seguinte:

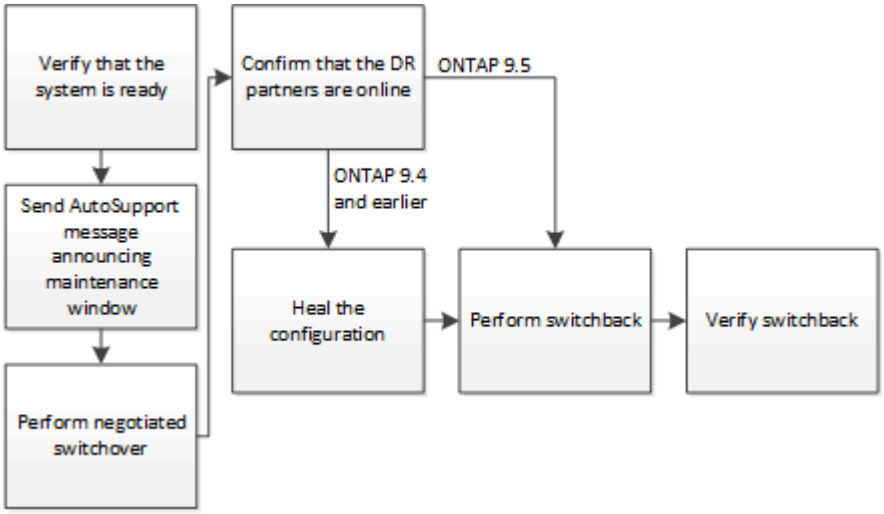
- Exclui os SVMs correspondentes no local do parceiro (o antigo local de desastre).
- Exclui quaisquer relações de peering dos SVMs excluídos.

Execute switchover, cura e switchback

Execute o switchover para testes ou manutenção

Realização de comutação para testes ou manutenção

Se quiser testar a funcionalidade do MetroCluster ou executar a manutenção planejada, você pode executar um switchover negociado no qual um cluster é colocado de forma limpa para o cluster de parceiros. Você pode então curar e voltar a configuração.



A partir do ONTAP 9.6, as operações de comutação e switchback podem ser executadas em configurações IP do MetroCluster com o Gerenciador de sistemas do ONTAP.

Limitações quando a configuração do MetroCluster está em switchover

Quando o sistema está em mudança, certas operações não devem ser executadas. Saiba mais sobre operações restritas quando o sistema está em switchover.

Operações restritas em switchover

As seguintes operações não são suportadas quando o sistema está em switchover:

- Criar ou excluir agregados e volumes
- Criando ou excluindo SVMs
- Criando ou excluindo LIFs
- Adicionar ou remover discos (somente se você estiver substituindo-os como parte de um procedimento de recuperação)
- Realizar alterações de configuração no SnapMirror SVM DR
- Modificar domínios de broadcast existentes ou criar novos domínios de broadcast
- Modificação de sub-redes de rede

Substituição de hardware em switchover

Use os seguintes procedimentos para substituir o hardware do controlador quando o sistema estiver em switchover:

- Se você precisar substituir um controlador do mesmo tipo, no local que não está em switchover, siga o procedimento para "Recuperar de uma falha de vários controladores ou armazenamento".
  - Se for necessário substituir os módulos do controlador e o chassis enquanto os nós estiverem comutados no local que sobrevive, encerre ambos os controladores e execute o procedimento para "Recuperar de uma falha de vários controladores ou armazenamento".
- Se for necessário substituir um controlador por um tipo diferente de controlador, siga o procedimento para a sua configuração no "Escolha um procedimento de atualização da controladora".
  - Se o seu sistema estiver em switchover devido a uma falha no controlador ou se você tiver uma falha no controlador durante o switchover, você deve primeiro substituir o hardware do controlador, executar um switchback e, em seguida, executar uma atualização do controlador:
    i. Para substituir o hardware do controlador e executar o switchback, siga "Recuperar de uma falha de vários controladores ou armazenamento".
    ii. Depois de substituir o hardware, execute uma atualização da controladora usando os procedimentos descritos no "Escolha um procedimento de atualização da controladora".

Verificar se o seu sistema está pronto para um switchover

Você pode usar a `-simulate` opção para visualizar os resultados de uma operação de switchover. Uma verificação fornece uma maneira de verificar se a maioria das pré-condições para uma execução bem-sucedida são atendidas antes de iniciar a operação. Emita estes comandos do site que permanecerão ativos e operacionais:

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. A partir do local que permanecerá ativo e operacional, simule uma operação de switchover: `metrocluster switchover -simulate`
3. Revise a saída que é retornada.

   A saída mostra se algum vetos evitaria uma operação de comutação. Toda vez que você executar uma operação MetroCluster, você deve verificar um conjunto de critérios para o sucesso da operação. Um "ponto" é um mecanismo que proíbe a operação se um ou mais critérios não forem cumpridos. Existem dois tipos de veto: Um veto "suave" e um veto "duro". Você pode substituir um veto suave, mas não um veto difícil. Por exemplo, para executar um switchover negociado em uma configuração de MetroCluster de quatro nós, um critério é que todos os nós estão ativos e íntegros. Suponha que um nó esteja inativo e tenha sido tomado por seu parceiro de HA. A operação de comutação será fortemente vetada porque é um critério difícil que todos os nós devem estar ativos e saudáveis. Porque este é um veto difícil, você não pode substituir o veto.

   ⓘ É melhor não substituir nenhum veto.

Exemplo: Resultados da verificação

O exemplo a seguir mostra os erros encontrados em uma simulação de uma operação de comutação:

```
cluster4::*> metrocluster switchover -simulate

[Job 126] Preparing the cluster for the switchover operation...
[Job 126] Job failed: Failed to prepare the cluster for the switchover
operation. Use the "metrocluster operation show" command to view detailed
error
information. Resolve the errors, then try the command again.
```

O switchover negociado e o switchback falharão até que você substitua todos os discos com falha. Você pode executar a recuperação de desastres depois de substituir os discos com falha. Se você quiser ignorar o aviso para discos com falha, você pode adicionar um veto suave para o switchover negociado e switchback.

Envio de uma mensagem AutoSupport personalizada antes do switchover negociado

Antes de executar um switchover negociado, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. O switchover negociado pode resultar em falhas de operação Plex ou MetroCluster que acionam mensagens AutoSupport. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Faça login no cluster em Site_A.
2. Chame uma mensagem AutoSupport indicando o início da manutenção: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

   especifica a duração da janela de manutenção e pode ser um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, pode emitir um comando para indicar que o período de manutenção terminou:`system node autosupport invoke -node * -type all -message MAINT=end`

3. Repita esta etapa no site do parceiro.

Realização de um switchover negociado

Um switchover negociado desliga os processos no local do parceiro de forma limpa e, em seguida, alterna as operações do local do parceiro. Você pode usar um switchover negociado para executar a manutenção em um local de MetroCluster ou para testar a funcionalidade de switchover.

- Todas as alterações de configuração anteriores devem ser concluídas antes de executar uma operação de switchback.

  Isto destina-se a evitar a concorrência com a operação de comutação negociada ou de comutação.

- Todos os nós que foram anteriormente inativos devem ser inicializados e no quorum de cluster.

  A *Referência da Administração do sistema* tem mais informações sobre o quórum de cluster na seção ""compreendendo quórum e epsilon"".

  "Administração do sistema"

- A rede de peering de cluster deve estar disponível em ambos os sites.
- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do software ONTAP.
- A opção replication.create_data_protection_rels.enable deve ser definida como ON EM ambos os sites em uma configuração MetroCluster antes de criar uma nova relação SnapMirror.
- Para uma configuração de MetroCluster de dois nós, uma nova relação do SnapMirror não deve ser criada durante uma atualização quando houver versões incompatíveis do ONTAP entre os sites.
- Para uma configuração de MetroCluster de quatro nós, as versões incompatíveis do ONTAP entre os sites não são suportadas.

O local de recuperação pode levar algumas horas para ser capaz de executar a operação de switchback.

O comando MetroCluster switchover alterna entre os nós em todos os grupos de DR na configuração MetroCluster. Por exemplo, em uma configuração de MetroCluster de oito nós, ele alterna entre os nós em ambos os grupos de DR.

Ao se preparar e executar um switchover negociado, você não deve fazer alterações de configuração no cluster nem executar nenhuma takeover ou operações de giveback.

Para configurações de MetroCluster FC:

- Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
- Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

Para configurações IP do MetroCluster:

> Antes de executar tarefas de manutenção, você deve remover o monitoramento se a configuração do MetroCluster for monitorada com o utilitário tiebreaker ou Mediator. "Remova a monitorização do Mediador ONTAP ou do tiebreaker antes de executar tarefas de manutenção"

- Para o ONTAP 9.4 e versões anteriores:
  - Os agregados espelhados ficarão degradados após o switchover negociado.
- Para o ONTAP 9.5 e posterior:
  - Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
  - Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Para o ONTAP 9.8 e posterior:
  - Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

i. Use os comandos MetroCluster check run, MetroCluster check show e MetroCluster check config-replication show para garantir que nenhuma atualização de configuração esteja em andamento ou pendente. Emita estes comandos do site que permanecerão ativos e operacionais.

ii. A partir do local que permanecerá ativo e operacional, implemente a transição: `metrocluster switchover`

A operação pode levar vários minutos para ser concluída.

iii. Monitorize a conclusão da mudança: `metrocluster operation show`

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

iv. Restabelecer qualquer configuração SnapMirror ou SnapVault.

Verifique se os SVMs estão em execução e se os agregados estão online

Após a conclusão do switchover, você deve verificar se os parceiros de DR se apropriaram dos discos e se os SVMs do parceiro se tornaram online.

Quando você executa o comando storage Aggregate plex show após um switchover do MetroCluster, o status de plex0 do agregado de raiz comutada é indeterminado e é exibido como falhou. Durante este tempo, a raiz comutada não é atualizada. O estado real deste Plex só pode ser determinado após a fase de cicatrização do MetroCluster.

Passos

1. Verifique se os agregados foram comutados usando o comando storage Aggregate show.

   Neste exemplo, os agregados foram trocados. O agregado raiz (aggr0_B2) está em um estado degradado. O agregado de dados (B2_aggr2) está em um estado espelhado e normal:

```
cluster_A::*> storage aggregate show

.
.
.
mcc1-b Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b2    227.1GB   45.1GB    80% online       0 node_A_1
raid_dp,

mirror

degraded
b2_aggr1    227.1GB   200.3GB    20% online       0 node_A_1
raid_dp,

mirrored

normal
```

2. Confirme se os SVMs secundários estão online usando o comando vserver show.

   Neste exemplo, os SVMs de destino de sincronização anteriormente adormecidos no site secundário foram ativados e têm um estado de administração em execução:

```
cluster_A::*> vserver show
                                          Admin      Operational  Root
Name    Name
Vserver           Type  Subtype           State      State        Volume
Aggregate  Service Mapping
-----------       ----- ----------        ---------- -----------
--------- ---------- ------- -------
...
cluster_B-vs1b-mc data   sync-destination  running   running
vs1b_vol   aggr_b1   file    file
```

Curar a configuração

Curar a configuração em uma configuração do MetroCluster FC

Cura da configuração em uma configuração de MetroCluster FC

Após um switchover, você deve executar as operações de recuperação de modo específico para restaurar o recurso de MetroCluster.

- O switchover deve ter sido realizado e o local sobrevivente deve estar fornecendo dados.
- Os nós no local de desastre devem ser interrompidos ou permanecer desligados.

  Eles não devem ser totalmente inicializados durante o processo de cura.

- O storage no local de desastre deve estar acessível (as prateleiras são ativadas, funcionais e acessíveis).
- Nas configurações MetroCluster conetadas à malha, os links entre switches (ISLs) devem estar ativos e operacionais.
- Em configurações de MetroCluster de quatro nós, os nós do local que sobrevive não devem estar no estado de failover de HA (todos os nós precisam estar ativos e em execução para cada par de HA).

A operação de recuperação deve primeiro ser realizada nos agregados de dados e, em seguida, nos agregados de raiz.

Recuperação dos agregados de dados após o switchover negociado

Você precisa curar os agregados de dados após concluir qualquer manutenção ou teste. Esse processo ressincroniza os agregados de dados e prepara o local de desastre para operação normal. Você precisa curar os agregados de dados antes de curar os agregados de raiz.

Todas as atualizações de configuração no cluster remoto replicam com sucesso para o cluster local. Você liga o storage no local de desastre como parte deste procedimento, mas não deve nem ligar os módulos do controlador no local de desastre.

Passos

1. Certifique-se de que o switchover foi concluído executando o comando MetroCluster operation show.

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. Ressincronize os agregados de dados executando o comando MetroCluster heal -phase agreements do cluster sobrevivente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   Se a cura for vetada, você terá a opção de reemitir o comando MetroCluster heal com o parâmetro --override-vetos. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software

que impeçam a operação de recuperação.

3. Verifique se a operação foi concluída executando o comando MetroCluster operation show.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Verifique o estado dos agregados executando o comando storage Aggregate show.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

5. Se o storage tiver sido substituído no local de desastre, talvez seja necessário espelhar novamente os agregados.

Recuperação dos agregados raiz após o switchover negociado

Depois que os agregados de dados tiverem sido curados, você deve curar os agregados de raiz em preparação para a operação de switchback.

A fase de agregados de dados do processo de recuperação do MetroCluster deve ter sido concluída com sucesso.

Passos

1. Alterne de volta os agregados espelhados executando o comando MetroCluster heal -phase root-aggregates.

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

   Se a cura for vetada, você terá a opção de reemitir o comando MetroCluster heal com o parâmetro --override-vetos. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

2. Confirme se a operação de cura está concluída executando o comando MetroCluster operation show no cluster saudável:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2014 20:54:41
   End Time: 7/29/2014 20:54:42
     Errors: -
```

3. Verifique e remova quaisquer discos com falha pertencentes ao local de desastre, emitindo o seguinte comando no local de integridade: `disk show -broken`
4. Ligue ou inicialize cada módulo do controlador no local de desastre.

   Se o sistema exibir o prompt Loader, execute o `boot_ontap` comando.

5. Depois que os nós forem inicializados, verifique se os agregados de raiz são espelhados.

   Se ambos os plexos estiverem presentes, a ressincronização ocorrerá automaticamente se os plexos não forem sincronizados. Se um Plex tiver falhado, esse Plex deve ser destruído e o espelho deve ser recriado usando o comando storage agred mirror -aggregate-name para restabelecer a relação de espelho.

Recuperação da configuração em uma configuração IP do MetroCluster (ONTAP 9 .4 e anterior)

Você deve curar os agregados em preparação para a operação de switchback.

Em sistemas IP MetroCluster que executam o ONTAP 9.5, a recuperação é executada automaticamente e você pode ignorar essas tarefas.

As seguintes condições devem existir antes de executar o procedimento de cicatrização:

- O switchover deve ter sido realizado e o local sobrevivente deve estar fornecendo dados.
- Os compartimentos de storage no local de desastre devem ser ativados, funcionais e acessíveis.
- Os ISLs devem estar ativos e operacionais.
- Os nós no local que sobrevive não devem estar no estado de failover de HA (ambos os nós precisam estar ativos e em execução).

Esta tarefa aplica-se apenas às configurações IP do MetroCluster que executam versões do ONTAP anteriores a 9,5.

Esse procedimento difere do procedimento de recuperação para configurações do MetroCluster FC.

Passos

1. Ligue cada módulo do controlador no site que foi comutado e deixe-os arrancar completamente.

   Se o sistema exibir o prompt Loader, execute o `boot_ontap` comando.

2. Execute a fase de recuperação de agregado de raiz: `metrocluster heal root-aggregates`

```
cluster_A::> metrocluster heal root-aggregates
[Job 137] Job succeeded: Heal Root-Aggregates is successful
```

Se a recuperação for vetada, você terá a opção de reemitir o comando MetroCluster heal root-agreements com o parâmetro --override-vetos. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

3. Ressincronizar os agregados: `metrocluster heal aggregates`

```
cluster_A::> metrocluster heal aggregates
[Job 137] Job succeeded: Heal Aggregates is successful
```

Se a cura for vetada, você terá a opção de reemitir o comando MetroCluster heal com o parâmetro --override-vetos. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

4. Confirme se a operação de cura está concluída executando o comando MetroCluster operation show no cluster saudável:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2017 20:54:41
   End Time: 7/29/2017 20:54:42
     Errors: -
```

Executando um switchback

Depois de curar a configuração do MetroCluster, você pode executar a operação MetroCluster switchback. A operação de switchback do MetroCluster retorna a configuração ao seu estado operacional normal, com as máquinas virtuais de armazenamento de origem sincronizada (SVMs) no local de desastre ativas e fornecendo dados dos pools de discos locais.

- O cluster de desastres deve ter mudado com sucesso para o cluster sobrevivente.
- A recuperação deve ter sido realizada nos agregados de dados e raiz.
- Os nós de cluster sobreviventes não devem estar no estado de failover de HA (todos os nós precisam estar ativos e em execução para cada par de HA).
- Os módulos do controlador do local de desastre devem ser completamente inicializados e não no modo de aquisição de HA.
- O agregado raiz deve ser espelhado.
- Os links interswitches (ISLs) devem estar online.
- Todas as licenças necessárias devem ser instaladas no sistema.

a. Confirme se todos os nós estão no estado ativado: `metrocluster node show`

   O exemplo a seguir exibe os nós que estão no estado habilitado:

```
cluster_B::>  metrocluster node show

DR                        Configuration  DR
Group Cluster Node        State          Mirroring Mode
----- ------- ----------- -------------- ---------
--------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots
completed
              node_A_2    configured     enabled   heal roots
completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

b. Confirme se a ressincronização está concluída em todos os SVMs: `metrocluster vserver show`

c. Verifique se todas as migrações automáticas de LIF que estão sendo executadas pelas operações de recuperação foram concluídas com sucesso: `metrocluster check lif show`

d. Execute um switchback simulado para verificar se o sistema está pronto: `metrocluster switchback -simulate`

e. Verificar a configuração:

   `metrocluster check run`

   O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results.
To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show
Last Checked On: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 entries were displayed.
```

f. Execute o switchback executando o comando MetroCluster switchback de qualquer nó no cluster sobrevivente: `metrocluster switchback`

g. Verifique o progresso do funcionamento do interrutor de comutação: `metrocluster show`

A operação de switchback ainda está em andamento quando a saída exibe Waiting-for-switchback:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

A operação de comutação está concluída quando a saída exibe normal:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

+
Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em

andamento usando o `metrocluster config-replication resync-status show` comando. Este comando está no nível de privilégio avançado.

a. Restabelecer qualquer configuração SnapMirror ou SnapVault.

   No ONTAP 8,3, você precisa restabelecer manualmente uma configuração de SnapMirror perdida após uma operação de switchback MetroCluster. No ONTAP 9.0 e mais tarde, o relacionamento é restabelecido automaticamente.

Verificando um switchback bem-sucedido

Depois de executar o switchback, você deseja confirmar que todos os agregados e máquinas virtuais de storage (SVMs) são trocados de volta e on-line.

1. Verifique se os agregados de dados comutados estão invertidos:

   `storage aggregate show`

   No exemplo a seguir, aggr_B2 no nó B2 mudou de volta:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal
```

2. Verifique se todos os SVMs de destino de sincronização no cluster sobrevivente estão inativos (mostrando um estado operacional "coberto"):

   `vserver show -subtype sync-destination`

```
node_B_1::> vserver show -subtype sync-destination
                                 Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                               running    stopped    vs1a_vol   aggr_b2
```

Os agregados de sincronização de destino na configuração MetroCluster têm o sufixo "'-mc" automaticamente anexado ao seu nome para ajudar a identificá-los.

3. Verifique se os SVMs de origem sincronizada no cluster de desastres estão ativos e em execução:

   `vserver show -subtype sync-source`

```
node_A_1::> vserver show -subtype sync-source
                                  Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                  running  running    vs1a_vol  aggr_b2
```

4. Confirme se as operações de switchback foram bem-sucedidas usando o `metrocluster operation show` comando.

Se o comando output mostrar…	Então…
Que o estado de operação de comutação é bem-sucedido.	O processo de switchback está concluído e você pode prosseguir com a operação do sistema.
Que a operação de switchback ou switchback-continuation-Agent é parcialmente bem-sucedida.	Execute a correção sugerida fornecida na saída do `metrocluster operation show` comando.

Você deve repetir as seções anteriores para executar o switchback na direção oposta. Se o site_A fez um switchover do site_B, faça um switchover do site_A.

Comandos para switchover, cura e switchback

Existem comandos ONTAP específicos para executar os processos de recuperação de desastres do MetroCluster.

Se você quiser…	Use este comando…
Verifique se o switchover pode ser executado sem erros ou vetos.	`metrocluster switchover -simulate` no nível de privilégio avançado
Verifique se o switchback pode ser executado sem erros ou vetos.	`metrocluster switchback -simulate` no nível de privilégio avançado
Alterne para os nós do parceiro (switchover negociado).	`metrocluster switchover`

Alterne para os nós de parceiros (switchover forçado).	`metrocluster switchover -forced-on-disaster true`
Executar a recuperação de agregado de dados.	`metrocluster heal -phase aggregates`
Executar a recuperação de agregado de raiz.	`metrocluster heal -phase root-aggregates`
Volte para os nós iniciais.	`metrocluster switchback`

Use o Gerenciador do sistema para executar o switchover e o switchback (somente configurações MetroCluster IP)

Você pode alternar o controle de um site IP do MetroCluster para o outro para executar a manutenção ou recuperar de um problema.

Os procedimentos de comutação e switchback são suportados apenas para configurações IP do MetroCluster.

Visão geral do switchover e do switchback

Um switchover pode ocorrer em duas instâncias:

- * Uma mudança planejada*

  Este switchover é iniciado por um administrador de sistema usando o System Manager. O switchover planejado permite que um administrador de sistema de um cluster local alterne o controle para que os serviços de dados do cluster remoto sejam gerenciados pelo cluster local. Em seguida, um administrador de sistema no local do cluster remoto pode executar a manutenção no cluster remoto.

- * Uma mudança não planejada*

  Em alguns casos, quando um cluster do MetroCluster cai ou as conexões entre os clusters estão inativas, o ONTAP inicia automaticamente um switchover para que o cluster que ainda está em execução gerencie as responsabilidades de gerenciamento de dados do cluster inativo.

  Em outras ocasiões, quando o ONTAP não consegue determinar o status de um dos clusters, o administrador do sistema do local que está trabalhando inicia o switchover para assumir o controle das responsabilidades de manuseio de dados do outro local.

Para qualquer tipo de procedimento de comutação, a capacidade de manutenção de dados é retornada ao cluster usando um processo *switchback*.

Você executa diferentes processos de comutação e switchback para ONTAP 9.7 e 9,8:

- Use o Gerenciador de sistemas no ONTAP 9.7 para comutação e switchback
- Use o Gerenciador de sistemas no ONTAP 9.8 para comutação e switchback

Use o Gerenciador de sistemas no ONTAP 9.7 para comutação e switchback

Passos

1. Inicie sessão no Gestor de sistema no ONTAP 9.7.
2. Clique em **(retornar à versão clássica)**.
3. Clique em **Configuração > MetroCluster**.

   O System Manager verifica se um switchover negociado é possível.

4. Execute uma das seguintes subetapas quando o processo de validação for concluído:
   a. Se a validação falhar, mas o local B estiver ativo, ocorreu um erro. Por exemplo, pode haver um problema com um subsistema ou o espelhamento do NVRAM pode não estar sincronizado.
      i. Corrija o problema que está causando o erro, clique em **Fechar** e, em seguida, inicie novamente na Etapa 2.
      ii. Interrompa os nós do local B, clique em **Fechar** e execute as etapas em "Executar um switchover não planejado".
   b. Se a validação falhar e o local B estiver inativo, é provável que haja um problema de conexão. Verifique se o local B está inativo e, em seguida, execute as etapas em "Executar um switchover não planejado".
5. Clique em **mudança do local B para o local A** para iniciar o processo de mudança.
6. Clique em **mudar para a nova experiência**.

Use o Gerenciador de sistemas no ONTAP 9.8 para comutação e switchback

Executar um switchover planejado (ONTAP 9.8)

Passos

1. Inicie sessão no Gestor de sistema no ONTAP 9.8.
2. Selecione **Painel**. Na seção **MetroCluster**, os dois clusters são mostrados com uma conexão.
3. No cluster local (mostrado à esquerda), clique em e selecione **mudar serviços de dados remotos para o local**.

   Após a validação da solicitação de switchover, o controle é transferido do local remoto para o local local. O local executa solicitações de serviço de dados para ambos os clusters.

   O cluster remoto reinicializa, mas os componentes de armazenamento não estão ativos e o cluster não atende solicitações de dados. Está agora disponível para manutenção planeada.

> O cluster remoto não deve ser usado para manutenção de dados até que você execute um switchback.

Executar um switchover não planejado (ONTAP 9.8)

Um switchover não planejado pode ser iniciado automaticamente pelo ONTAP. Se o ONTAP não puder determinar se um switchback é necessário, o administrador do sistema do local do MetroCluster que ainda está em execução iniciará o switchover com as seguintes etapas:

Passos

1. Inicie sessão no Gestor de sistema no ONTAP 9.8.
2. Selecione **Painel**.

   Na seção **MetroCluster**, a conexão entre os dois clusters é mostrada com um "X" nele. Isso significa que não é possível detetar uma conexão e que as conexões ou o cluster estão inoperantes.

3. No cluster local (mostrado à esquerda), clique ⋮ em e selecione **mudar serviços de dados remotos para o local**.

   Se o switchover falhar com um erro, clique no link "Exibir detalhes" na mensagem de erro e confirme o switchover não planejado.

   Após a validação da solicitação de switchover, o controle é transferido do local remoto para o local local. O local executa solicitações de serviço de dados para ambos os clusters.

   O cluster deve ser reparado antes de ser colocado online novamente.

ⓘ Depois que o cluster remoto for colocado on-line, ele não deve ser usado para manutenção de dados até que você execute um switchback.

Executar um switchback (ONTAP 9.8)

Antes de começar

Se o cluster remoto estava inativo devido a manutenção planejada ou devido a um desastre, ele agora deve estar funcionando e aguardando o switchback.

Passos

1. No cluster local, inicie sessão no Gestor do sistema no ONTAP 9.8.
2. Selecione **Painel**.

   Na seção **MetroCluster**, os dois clusters são exibidos.

3. No cluster local (mostrado à esquerda), clique ⋮ em e selecione **Take Back control**.

   Os dados são *curados* primeiro, para verificar se os dados estão sincronizados e espelhados entre ambos os clusters.

4. Quando a recuperação de dados estiver concluída, clique ⋮ em e selecione **Iniciar switchback**.

   Quando o switchback estiver concluído, ambos os clusters estão ativos e atendem às solicitações de dados. Além disso, os dados estão sendo espelhados e sincronizados entre os clusters.

Monitorização da configuração do MetroCluster

Você pode usar os comandos do ONTAP MetroCluster e o Active IQ Unified Manager (anteriormente Gerenciador Unificado do OnCommand) para monitorar a integridade de vários componentes de software e o estado das operações do MetroCluster.

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente. Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster. Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Sobre esta tarefa

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Os comandos subsequentes `metrocluster check show` não mostram a saída esperada.

Passos

1. Verificar a configuração:

   `metrocluster check run`

   O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

2. Exibir resultados mais detalhados do comando mais recente `metrocluster check run`:

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`

   `metrocluster check node show`

   Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

   O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

   ```
   cluster_A::> metrocluster check aggregate show
   ```

```
Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr2
                                                mirroring-status
ok
```

```
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

O exemplo a seguir mostra a `metrocluster check cluster show` saída do comando para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

Comandos para verificar e monitorar a configuração do MetroCluster

Existem comandos ONTAP específicos para monitorar a configuração do MetroCluster e verificar as operações do MetroCluster.

Comandos para verificar as operações do MetroCluster

Se você quiser…	Use este comando…
Efetue uma verificação das operações do MetroCluster. **Nota:** este comando não deve ser usado como o único comando para validação do sistema de operação pré-DR.	`metrocluster check run`

Veja os resultados da última verificação das operações do MetroCluster.	`metrocluster show`
Veja os resultados da verificação na replicação de configuração entre os sites.	`metrocluster check config-replication show metrocluster check config-replication show-aggregate-eligibility`
Veja os resultados da verificação na configuração do nó.	`metrocluster check node show`
Veja os resultados da verificação na configuração agregada.	`metrocluster check aggregate show`
Veja as falhas de colocação de LIF na configuração do MetroCluster.	`metrocluster check lif show`

Comandos para monitorar a interconexão MetroCluster

Se você quiser…	Use este comando…
Exibir o status e as informações do espelhamento de HA e DR para os nós MetroCluster no cluster.	`metrocluster interconnect mirror show`

Comandos para monitorar SVMs MetroCluster

Se você quiser…	Use este comando…
Veja todos os SVMs em ambos os locais na configuração do MetroCluster.	`metrocluster vserver show`

Usando o tiebreaker MetroCluster ou o Mediador ONTAP para monitorar a configuração

"Diferenças entre ONTAP Mediator e MetroCluster tiebreaker"Consulte para compreender as diferenças entre estes dois métodos de monitorização da configuração do MetroCluster e de início de um switchover automático.

Use esses links para instalar e configurar tiebreaker ou Mediator:

- "Instale e configure o software tiebreaker do MetroCluster"
- "Prepare-se para instalar o serviço Mediador ONTAP"

Como o software tiebreaker do NetApp MetroCluster deteta falhas

O software tiebreaker reside em um host Linux. Você só precisa do software tiebreaker se quiser monitorar dois clusters e o status de conectividade entre eles em um terceiro local. Com isso, cada parceiro em um cluster pode diferenciar uma falha de ISL, quando os links entre locais estão inativos, de uma falha do local.

Depois de instalar o software tiebreaker em um host Linux, é possível configurar os clusters em uma configuração do MetroCluster para monitorar as condições de desastre.

Como o software tiebreaker deteta falhas de conetividade entre sites

O software tiebreaker do MetroCluster alerta você se toda a conetividade entre os sites for perdida.

Tipos de caminhos de rede

Dependendo da configuração, existem três tipos de caminhos de rede entre os dois clusters em uma configuração MetroCluster:

- **Rede FC (presente em configurações MetroCluster conetadas à malha)**

  Esse tipo de rede é composto por duas malhas de switch FC redundantes. Cada malha de switch tem dois switches FC, com um switch de cada malha de switch colocado com um cluster. Cada cluster tem dois switches FC, um de cada malha de switch. Todos os nós têm conectividade FC (interconexão NV e iniciador FCP) a cada um dos switches IP colocalizados. Os dados são replicados de cluster para cluster através do ISL.

- **Rede de peering entre clusters**

  Este tipo de rede é composto por um caminho de rede IP redundante entre os dois clusters. A rede de peering de cluster fornece a conectividade necessária para espelhar a configuração da máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada pelo cluster de parceiros.

- **Rede IP (presente nas configurações IP do MetroCluster)**

  Este tipo de rede é composto por duas redes de switch IP redundantes. Cada rede tem dois switches IP, com um switch de cada malha de switch co-localizado com um cluster. Cada cluster tem dois switches IP, um de cada malha de switch. Todos os nós têm conectividade a cada um dos switches FC colocalizados. Os dados são replicados de cluster para cluster através do ISL.

Monitoramento da conetividade entre sites

O software tiebreaker recupera regularmente o status da conetividade entre sites dos nós. Se a conetividade de interconexão NV for perdida e o peering entre clusters não responder a pings, os clusters assumem que os sites estão isolados e o software tiebreaker aciona um alerta como "AllLinksSevered". Se um cluster identificar o status "AllLinksSevered" e o outro cluster não estiver acessível através da rede, o software tiebreaker aciona um alerta como "desastre".

Como o software tiebreaker deteta falhas no local

O software tiebreaker do NetApp MetroCluster verifica a acessibilidade dos nós em uma configuração do MetroCluster e do cluster para determinar se ocorreu uma falha no local. O software tiebreaker também aciona um alerta sob certas condições.

Componentes monitorados pelo software tiebreaker

O software tiebreaker monitora cada controladora na configuração do MetroCluster estabelecendo conexões redundantes por meio de vários caminhos para um LIF de gerenciamento de nós e para o LIF de gerenciamento de cluster, ambos hospedados na rede IP.

O software tiebreaker monitora os seguintes componentes na configuração do MetroCluster:

- Nós por meio de interfaces de nós locais
- Cluster por meio das interfaces designadas por cluster
- Cluster sobrevivente para avaliar se ele tem conetividade com o local de desastre (interconexão NV, armazenamento e peering entre clusters)

Quando houver uma perda de conexão entre o software tiebreaker e todos os nós no cluster e para o próprio cluster, o cluster será declarado como "não alcançável" pelo software tiebreaker. Demora cerca de três a cinco segundos para detetar uma falha de ligação. Se um cluster não estiver acessível a partir do software tiebreaker, o cluster sobrevivente (o cluster que ainda está acessível) deve indicar que todos os links para o cluster de parceiros são cortados antes que o software tiebreaker acione um alerta.

Todos os links são cortados se o cluster sobrevivente não puder mais se comunicar com o cluster no local de desastre por meio de FC (interconexão e armazenamento NV) e peering entre clusters.

Cenários de falha durante os quais o software tiebreaker aciona um alerta

O software tiebreaker aciona um alerta quando o cluster (todos os nós) no local de desastre está inativo ou inacessível e o cluster no local sobrevivente indica o status "AllLinksSevered".

O software tiebreaker não aciona um alerta (ou o alerta é vetado) nos seguintes cenários:

- Em uma configuração de MetroCluster de oito nós, se um par de HA no local de desastre estiver inativo
- Em um cluster com todos os nós no local do desastre para baixo, um par de HA no local sobrevivente para baixo, e o cluster no local sobrevivente indica o status "AllLinksSevered"

  O software tiebreaker aciona um alerta, mas o ONTAP veta esse alerta. Nesta situação, também é vetado um switchover manual

- Qualquer cenário em que o software tiebreaker possa alcançar pelo menos um nó ou a interface de cluster no local de desastre, ou o local sobrevivente ainda pode alcançar qualquer nó no local de desastre por meio de FC (interconexão e storage NV) ou peering entre clusters

Como o Mediador ONTAP suporta o switchover não planejado automático

"Saiba mais sobre como o Mediador ONTAP suporta o switchover não planejado automático em configurações IP do MetroCluster".

Monitoramento e proteção da consistência do sistema de arquivos usando NVFAIL

O `-nvfail` parâmetro `volume modify` do comando permite que o ONTAP detete inconsistências de RAM não volátil (NVRAM) quando o sistema está inicializando ou após uma operação de comutação. Ele também avisa e protege o sistema contra acesso e modificação de dados até que o volume possa ser recuperado manualmente.

Se o ONTAP detetar algum problema, as instâncias de banco de dados ou sistema de arquivos param de responder ou desligar. Em seguida, o ONTAP envia mensagens de erro para o console para alertá-lo para verificar o estado do banco de dados ou do sistema de arquivos. Você pode habilitar o NVFAIL para avisar os administradores de banco de dados sobre inconsistências do NVRAM entre nós em cluster que podem comprometer a validade do banco de dados.

Após a perda de dados do NVRAM durante a recuperação de failover ou inicialização, os clientes NFS não podem acessar dados de nenhum dos nós até que o estado NVFAIL seja limpo. Os clientes CIFS não são afetados.

Como o NVFAIL afeta o acesso a volumes NFS ou LUNs

O estado NVFAIL é definido quando o ONTAP deteta erros NVRAM durante a inicialização, quando ocorre uma operação de comutação MetroCluster ou durante uma operação de aquisição de HA se a opção NVFAIL estiver definida no volume. Se nenhum erro for detetado na inicialização, o serviço de arquivos é iniciado normalmente. No entanto, se erros do NVRAM forem detetados ou o processamento NVFAIL for aplicado em um switchover de desastre, o ONTAP interrompe as instâncias do banco de dados de responder.

Quando você ativa a opção NVFAIL, um dos processos descritos na tabela a seguir ocorre durante a inicialização:

Se…	Então…
O ONTAP não deteta erros de NVRAM	O serviço de arquivos é iniciado normalmente.
O ONTAP deteta erros do NVRAM	• O ONTAP retorna um erro de identificador de arquivo obsoleto (ESTALE) para clientes NFS que tentam acessar o banco de dados, fazendo com que o aplicativo pare de responder, travar ou desligar. Em seguida, o ONTAP envia uma mensagem de erro para o console do sistema e arquivo de log. • Quando o aplicativo é reiniciado, os arquivos ficam disponíveis para clientes CIFS, mesmo que você não tenha verificado que eles são válidos. Para clientes NFS, os arquivos permanecem inacessíveis até que você redefina `in-nvfailed-state` a opção no volume afetado.
Se for utilizado um dos seguintes parâmetros: • `dr-force-nvfail` a opção volume está definida • `force-nvfail-all` a opção de comando de comutação está definida.	Você pode desmarcar a `dr-force-nvfail` opção após o switchover, se o administrador não estiver esperando forçar o processamento NVFAIL para possíveis operações futuras de switchover de desastre. Para clientes NFS, os arquivos permanecem inacessíveis até que você redefina `in-nvfailed-state` a opção no volume afetado. O uso da `force-nvfail-all` opção faz com que a `dr-force-nvfail` opção seja definida em todos os volumes de DR processados durante o switchover de desastre.

O ONTAP deteta erros do NVRAM em um volume que contém LUNs	Os LUNs nesse volume são colocados offline. A `in-nvfailed-state` opção no volume deve ser limpa e o atributo NVFAIL nos LUNs deve ser limpo colocando cada LUN no volume afetado on-line. Você pode executar as etapas para verificar a integridade dos LUNs e recuperar o LUN de uma cópia Snapshot ou backup, conforme necessário. Depois que todos os LUNs no volume forem recuperados, a `in-nvfailed-state` opção no volume afetado será limpa.

Comandos para monitorar eventos de perda de dados

Se você ativar a opção NVFAIL, receberá uma notificação quando ocorrer uma falha do sistema causada por inconsistências do NVRAM ou um switchover do MetroCluster.

Por padrão, o parâmetro NVFAIL não está habilitado.

Se você quiser…	Use este comando…
Crie um novo volume com NVFAIL ativado	`volume create -nvfail on`
Ative NVFAIL em um volume existente	`volume modify` **Nota:** você define a `-nvfail` opção como "On" para ativar o NVFAIL no volume criado.
Indique se o NVFAIL está atualmente ativado para um volume especificado	`volume show` **Nota:** você define o `-fields` parâmetro como "nvfail" para exibir o atributo NVFAIL para um volume especificado.

Informações relacionadas

Consulte a página de manual de cada comando para obter mais informações.

Acessar volumes no estado NVFAIL após um switchover

Após um switchover, você deve limpar o estado NVFAIL redefinindo o `-in-nvfailed-state` parâmetro `volume modify` do comando para remover a restrição de clientes para acessar dados.

Antes de começar

O banco de dados ou o sistema de arquivos não deve estar em execução ou tentando acessar o volume afetado.

Sobre esta tarefa

A definição `-in-nvfailed-state` de parâmetro requer privilégios de nível avançado.

Passo

1. Recupere o volume usando o comando volume Modify com o parâmetro -in-nvfailed-State definido como false.

Depois de terminar

Para obter instruções sobre como examinar a validade do arquivo de banco de dados, consulte a documentação do seu software de banco de dados específico.

Se o banco de dados usar LUNs, revise as etapas para tornar os LUNs acessíveis ao host após uma falha do NVRAM.

Informações relacionadas

"Monitoramento e proteção da consistência do sistema de arquivos usando NVFAIL"

Recuperação de LUNs nos estados NVFAIL após o switchover

Após um switchover, o host não tem mais acesso aos dados nos LUNs nos estados NVFAIL. Você deve executar várias ações antes que o banco de dados tenha acesso aos LUNs.

Antes de começar

O banco de dados não deve estar em execução.

Passos

1. Limpe o estado NVFAIL no volume afetado que hospeda os LUNs redefinindo o `-in-nvfailed-state` parâmetro `volume modify` do comando.
2. Coloque online os LUNs afetados.
3. Examine os LUNs para encontrar inconsistências de dados e resolva-os.

   Isso pode envolver a recuperação baseada em host ou a recuperação feita no controlador de storage usando o SnapRestore.

4. Coloque o aplicativo de banco de dados on-line depois de recuperar os LUNs.

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Documentação do MetroCluster"	• Todas as informações do MetroCluster
"Relatório Técnico da NetApp 4375: NetApp MetroCluster for ONTAP 9.3"	• Uma visão geral técnica da configuração e operação do MetroCluster. • Práticas recomendadas para a configuração do MetroCluster.

"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Instalação e configuração IP do MetroCluster"	• Arquitetura IP do MetroCluster • Fazer o cabeamento da configuração • Configurando o MetroCluster no ONTAP
"Instalação e configuração do software MetroCluster tiebreaker 1,21"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
Documentação do Active IQ Unified Manager "Documentação do NetApp: Guias de produto e recursos"	• Monitoramento da configuração e do desempenho do MetroCluster
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster

Mantenha os componentes do MetroCluster

Prepare-se para a manutenção do MetroCluster

Ative o registo da consola antes de executar tarefas de manutenção

Ative o registo da consola nos seus dispositivos antes de executar tarefas de manutenção.

A NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações antes de executar os procedimentos de manutenção:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Remova a monitorização do Mediador ONTAP ou do tiebreaker antes de executar tarefas de manutenção

Antes de executar tarefas de manutenção, você deve remover o monitoramento se a configuração do MetroCluster for monitorada com o utilitário tiebreaker ou Mediator.

As tarefas de manutenção incluem a atualização da plataforma do controlador, a atualização do ONTAP e a execução de um switchover e um switchback negociado.

Passos

1. Colete a saída para o seguinte comando:

   ```
   storage iscsi-initiator show
   ```

2. Remova a configuração do MetroCluster existente do tiebreaker, Mediator ou outro software que possa iniciar o switchover.

Se você estiver usando…	Use este procedimento…
Desempate	"Remoção das configurações do MetroCluster" No *MetroCluster Tiebreaker Instalação e Configuração conteúdo*
Mediador	Execute o seguinte comando no prompt do ONTAP: `metrocluster configuration-settings mediator remove`

Aplicativos de terceiros	Consulte a documentação do produto.

3. Depois de concluir a manutenção da configuração do MetroCluster, você pode retomar o monitoramento com o utilitário tiebreaker ou Mediator.

Se você estiver usando…	Use este procedimento
Desempate	"Adição de configurações do MetroCluster" Na seção *MetroCluster tiebreaker Installation and Configuration*.
Mediador	"Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster" Na seção *Instalação e Configuração IP do MetroCluster*.
Aplicativos de terceiros	Consulte a documentação do produto.

Cenários de falha e recuperação do MetroCluster

Você deve estar ciente de como a configuração do MetroCluster responde a diferentes eventos de falha.

Para obter informações adicionais sobre a recuperação de falhas de nó, consulte a seção "escolher o procedimento de recuperação correto" no "Recuperar de um desastre".

Evento	Impacto	Recuperação
Falha de nó único	Um failover é acionado.	A configuração se recupera por meio de uma aquisição local. RAID não é afetado. Revise as mensagens do sistema e substitua as FRUs com falha, conforme necessário. "Documentação dos sistemas de hardware da ONTAP"
Dois nós falham em um local	Dois nós só falharão se o switchover automatizado for habilitado no software tiebreaker do MetroCluster.	Switchover não planejado manual (USO) se o switchover automatizado no software tiebreaker do MetroCluster não estiver ativado. "Documentação dos sistemas de hardware da ONTAP"

Interface IP MetroCluster - falha de uma porta	O sistema está degradado. Falha de porta adicional afeta o espelhamento de HA.	A segunda porta é usada. O Monitor de integridade gera um alerta se o link físico para a porta estiver quebrado. Revise as mensagens do sistema e substitua as FRUs com falha, conforme necessário. "Documentação dos sistemas de hardware da ONTAP"
Interface IP MetroCluster - falha de ambas as portas	A capacidade DE HA é afetada. O RAID SyncMirror do nó pára a sincronização.	É necessária uma recuperação manual imediata, uma vez que não existe uma aquisição de HA. Revise as mensagens do sistema e substitua as FRUs com falha, conforme necessário. "Documentação dos sistemas de hardware da ONTAP"
Falha de um switch IP MetroCluster	Sem impactos. A redundância é fornecida através da segunda rede.	Substitua o interrutor com falha, conforme necessário. "Substituição de um switch IP"
Falha de dois switches IP MetroCluster que estão na mesma rede	Sem impactos. A redundância é fornecida através da segunda rede.	Substitua o interrutor com falha, conforme necessário. "Substituição de um switch IP"
Falha de dois switches IP MetroCluster que estão em um local	O RAID SyncMirror do nó pára a sincronização. A capacidade DE HA é afetada e o cluster fica sem quorum.	Substitua o interrutor com falha, conforme necessário. "Substituição de um switch IP"
Falha de dois switches IP MetroCluster que estão em locais diferentes e não na mesma rede (falha diagonal)	O RAID SyncMirror do nó pára a sincronização.	O RAID SyncMirror do nó pára a sincronização. Os recursos de cluster e HA não são afetados. Substitua o interrutor com falha, conforme necessário. "Substituição de um switch IP"

Usando a ferramenta Matriz de interoperabilidade para encontrar informações do MetroCluster

Ao configurar a configuração do MetroCluster, você pode usar a ferramenta de interoperabilidade para garantir que está usando versões de software e hardware suportadas.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Depois de abrir a Matriz de interoperabilidade, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster.

Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa.

Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

Onde encontrar procedimentos para tarefas de manutenção do MetroCluster

Você deve ter certeza de que selecionou o procedimento correto quando executar tarefas de manutenção de hardware do MetroCluster.

Procedimentos de manutenção para diferentes tipos de configurações do MetroCluster

- Se tiver uma configuração IP do MetroCluster, reveja os procedimentos em "Procedimentos de manutenção para configurações IP do MetroCluster".
- Se tiver uma configuração MetroCluster FC, reveja os procedimentos em "Procedimentos de manutenção para configurações MetroCluster FC".
- Se não conseguir encontrar o procedimento na secção específica da sua configuração, reveja os procedimentos em "Procedimentos de manutenção para todas as configurações do MetroCluster".

Todos os outros procedimentos de manutenção

A tabela a seguir fornece links para procedimentos relacionados à manutenção do MetroCluster que não estão localizados nas três seções listadas acima:

Componente	Tipo MetroCluster (FC ou IP)	Tarefa	Procedimento
Software ONTAP	Ambos	Atualização do software ONTAP	"Atualize, reverta ou downgrade"

Módulo do controlador	Ambos	Substituição de FRU (incluindo módulos de controladora, placas PCIe, placa FC-VI e assim por diante) A movimentação de um módulo de controlador de armazenamento ou de uma placa NVRAM entre os sistemas de armazenamento MetroCluster não é suportada.	"Documentação dos sistemas de hardware da ONTAP"
Atualização e expansão	"Atualização e expansão do MetroCluster"	Transição da conectividade FC para IP	"Transição do MetroCluster FC para o MetroCluster IP"
Compartimento de unidades	FC	Todos os outros procedimentos de manutenção da prateleira. Os procedimentos padrão podem ser usados.	"Mantenha as gavetas de disco DS460C DS224C e DS212C"
IP	Todos os procedimentos de manutenção das prateleiras. Os procedimentos padrão podem ser usados. Se adicionar prateleiras para um agregado sem espelhamento, consulte "Considerações ao usar agregados sem espelhamento"	"Mantenha as gavetas de disco DS460C DS224C e DS212C"	Ambos

Procedimentos de manutenção para configurações MetroCluster FC

Modifique um endereço IP de switch ou ponte ATTO para monitoramento de integridade

Depois de modificar os endereços IP dos switches back-end MetroCluster FC e das bridges ATTO, você deve substituir os endereços IP de monitoramento de integridade antigos pelos novos valores.

- Modifique um endereço IP do switch
- Modifique um endereço IP de ponte ATTO

Modifique um endereço IP do switch

Substitua o antigo endereço IP de monitoramento de integridade de um switch back-end MetroCluster FC.

Antes de começar

Consulte a documentação do fornecedor do switch para o modelo do switch para alterar o endereço IP do switch antes de alterar o endereço IP de monitoramento de integridade.

Passos

1. Execute o `::> storage switch show` comando e na saída, observe os switches que estão relatando erros.
2. Remova as entradas do switch com endereços IP antigos:

   ```
   ::> storage switch remove -name switch_name
   ```

3. Adicione os switches com novos endereços IP:

   ```
   ::> storage switch add -name switch_name -address new_IP_address -managed-by
   in-band
   ```

4. Verifique os novos endereços IP e confirme se não existem erros:

   ```
   ::> storage switch show
   ```

5. Se necessário, atualize as entradas:

   ```
   ::> set advanced

   ::*> storage switch refresh

   ::*> set admin
   ```

Modifique um endereço IP de ponte ATTO

Substitua o antigo endereço IP de monitoramento de integridade de uma ponte ATTO.

Passos

1. Execute o `::> storage bridge show` comando e na saída, observe as bridges ATTO que estão relatando erros.
2. Remova as entradas da ponte ATTO com endereços IP antigos:

   ```
   ::> storage bridge remove -name ATTO_bridge_name
   ```

3. Adicione as bridges ATTO com novos endereços IP:

   ```
   ::> storage bridge add -name ATTO_bridge_name -address new_IP_address -managed
   -by in-band
   ```

4. Verifique os novos endereços IP e confirme se não existem erros:

   ```
   ::> storage bridge show
   ```

5. Se necessário, atualize as entradas:

   ```
   ::> set advanced

   ::*> storage bridge refresh

   ::*> set admin
   ```

Manutenção da ponte FC-para-SAS

Suporte para bridgeBridge 7600N em configurações MetroCluster

A ponte FibreBridge 7600N é suportada no ONTAP 9.5 e posterior como um substituto para a ponte FibreBridge 7500N ou 6500N ou ao adicionar novo armazenamento à configuração do MetroCluster. Os requisitos de zoneamento e restrições em relação ao uso dos portos FC da ponte são os mesmos que os da ponte FibreBridge 7500N.

"Ferramenta de Matriz de interoperabilidade do NetApp"

As bridges FibreBridge 6500N não são suportadas em configurações que executam o ONTAP 9.8 e posterior.

Caso de uso	Mudanças de zoneamento necessárias?	Restrições	Procedimento
Substituindo uma única ponte FibreBridge 7500N por uma única ponte FibreBridge 7600N	Não	A ponte FibreBridge 7600N deve ser configurada exatamente da mesma forma que a ponte FibreBridge 7500N.	"Troca quente de uma FibreBridge 7500N com uma ponte 7600N"

Substituindo uma única ponte FibreBridge 6500N por uma única ponte FibreBridge 7600N	Não	A ponte FibreBridge 7600N deve ser configurada exatamente da mesma forma que a ponte FibreBridge 6500N.	"Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N"
Adicionando um novo armazenamento através da adição de um novo par de pontes FibreBridge 7600N	Sim É necessário adicionar zonas de storage para cada uma das portas FC das novas pontes.	Você precisa ter portas disponíveis na malha do switch FC (em uma configuração MetroCluster conectada à malha) ou nos controladores de storage (em uma configuração Stretch MetroCluster). Cada par de pontes do FibreBridge 7500N ou 7600N pode oferecer suporte a até quatro stacks.	"Adição rápida de uma stack de shelves de disco SAS e bridges a um sistema MetroCluster"

Suporte para bridgeBridge 7500N em configurações MetroCluster

A ponte FibreBridge 7500N é suportada como um substituto para a ponte FibreBridge 6500N ou para ao adicionar novo armazenamento à configuração do MetroCluster. As configurações suportadas têm requisitos de zoneamento e restrições em relação ao uso das portas FC da ponte e dos limites de stack e shelf de armazenamento.

As bridges FibreBridge 6500N não são suportadas em configurações que executam o ONTAP 9.8 e posterior.

Caso de uso	Mudanças de zoneamento necessárias?	Restrições	Procedimento
Substituindo uma única ponte FibreBridge 6500N por uma única ponte FibreBridge 7500N	Não	A ponte FibreBridge 7500N deve ser configurada exatamente da mesma forma que a ponte FibreBridge 6500N, usando uma única porta FC e anexando a uma única pilha. A segunda porta FC no FibreBridge 7500N não deve ser usada.	"Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N"

Caso de uso	Mudanças de zoneamento necessárias?	Restrições	Procedimento
Consolidando várias pilhas substituindo vários pares de pontes FibreBridge 6500N por um único par de pontes FibreBridge 7500N	Sim	Neste caso, você tira as pontes FibreBridge 6500N fora de serviço e as substitui por um único par de pontes FibreBridge 7500N. Cada par de pontes FibreBridge 7500N ou 7600N pode suportar até quatro pilhas. No final do procedimento, tanto a parte superior como a parte inferior das pilhas devem ser conetadas às portas correspondentes nas pontes FibreBridge 7500N.	"Substituição de um par de pontes FibreBridge 6500N por pontes 7600N ou 7500N"
Adicionando um novo armazenamento através da adição de um novo par de pontes FibreBridge 7500N	Sim É necessário adicionar zonas de storage para cada uma das portas FC das novas pontes.	Você precisa ter portas disponíveis na malha do switch FC (em uma configuração MetroCluster conectada à malha) ou nos controladores de storage (em uma configuração Stretch MetroCluster). Cada par de pontes do FibreBridge 7500N ou 7600N pode oferecer suporte a até quatro stacks.	"Adição rápida de uma stack de shelves de disco SAS e bridges a um sistema MetroCluster"

Ativar o acesso à porta IP na ponte FibreBridge 7600N, se necessário

Se você estiver usando uma versão do ONTAP anterior a 9,5, ou de outra forma planeja usar o acesso fora da banda à ponte FibreBridge 7600N usando telnet ou outros protocolos e serviços de porta IP (FTP, ExpressNAV, ICMP ou Quicknav), você pode ativar os serviços de acesso através da porta do console.

Ao contrário da ponte ATTO FibreBridge 7500N, a ponte FibreBridge 7600N é fornecida com todos os protocolos e serviços de porta IP desativados.

A partir do ONTAP 9.5, *gerenciamento na banda* das bridges é suportado. Isso significa que as pontes podem ser configuradas e monitoradas a partir da CLI do ONTAP por meio da conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário e as interfaces do usuário da ponte não são necessárias.

A partir do ONTAP 9.8, *gerenciamento na banda* das bridges é suportado por padrão e o gerenciamento SNMP fora da banda é obsoleto.

Essa tarefa é necessária se você estiver usando **não** o gerenciamento na banda para gerenciar as bridges.

Neste caso, você precisa configurar a ponte através da porta de gerenciamento Ethernet.

Passos

1. Acesse a interface do console da ponte conetando um cabo serial à porta serial na ponte FibreBridge 7600N.
2. Usando o console, ative os serviços de acesso e salve a configuração:

   `set closeport none`

   `saveconfiguration`

   O `set closeport none` comando habilita todos os serviços de acesso na ponte.

3. Desative um serviço, se desejado, emitindo `set closeport` e repetindo o comando conforme necessário até que todos os serviços desejados sejam desativados:

   `set closeport *service*`

   O `set closeport` comando desativa um único serviço de cada vez.

   `service` pode especificar uma das seguintes opções:

   - expressarsnav
   - ftp
   - icmp
   - navegação rápida
   - snmp
   - telnet

     Pode verificar se um protocolo específico está ativado ou desativado utilizando o `get closeport` comando.

4. Se estiver a ativar o SNMP, também tem de emitir o comando Set SNMP enabled (Definir SNMP ativado):

   `set SNMP enabled`

   SNMP é o único protocolo que requer um comando de ativação separado.

5. Guardar a configuração:

   `saveconfiguration`

Atualizando o firmware em uma ponte FibreBridge

O procedimento para atualizar o firmware da ponte depende do modelo da ponte e da versão do ONTAP.

Sobre esta tarefa

"Ativar o registo da consola" antes de executar esta tarefa.

Atualização de firmware em bridgeBridge 7600N ou 7500N bridges em configurações executando o ONTAP 9.4 e posterior

Talvez seja necessário atualizar o firmware em suas bridges do FibreBridge para garantir que você tenha os recursos mais recentes ou para resolver possíveis problemas. Esse procedimento deve ser usado para pontes FibreBridge 7600N ou 7500N em configurações executando o ONTAP 9.4 e posterior.

- A configuração do MetroCluster deve estar funcionando normalmente.
- Todas as bridges do FibreBridge na configuração do MetroCluster devem estar ativas e operacionais.
- Todos os caminhos de armazenamento devem estar disponíveis.
- Você precisa da senha de administrador e acesso a um servidor HTTP, FTP, SFTP ou TFTP (Trivial File Transfer Protocol).
- Você deve estar usando uma versão de firmware suportada.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

  No IMT, você pode usar o campo solução de armazenamento para selecionar sua solução MetroCluster. Use o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode clicar em **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Você pode usar essa tarefa somente em bridges do FibreBridge 7600N ou 7500N em configurações executando o ONTAP 9.4 ou posterior.
- Você deve executar essa tarefa em cada bridge do FibreBridge na configuração do MetroCluster, para que todas as bridges estejam executando a mesma versão de firmware.

Esse procedimento não causa interrupções e leva aproximadamente 30 minutos para ser concluído.

A partir de ONTAP 9.8, o `system bridge` comando substitui o `storage bridge`. As etapas a seguir mostram o `system bridge` comando, mas se você estiver executando uma versão anterior ao ONTAP 9.8, você deve usar o `storage bridge` comando.

Passos

1. Chame uma mensagem AutoSupport indicando o início da manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   "manutenção-janela-em-horas" especifica o comprimento da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=end`

2. Vá para a página ATTO FibreBridge e selecione o firmware apropriado para a ponte.

   "Página de download do firmware do ATTO FibreBridge"

3. Reveja o Acordo de cuidado/MustRead e Utilizador final e clique na caixa de verificação para indicar a aceitação e prosseguir.

4. Coloque o arquivo de firmware em um local de rede acessível aos módulos do controlador.

   Você pode inserir os comandos nas etapas restantes a partir do console de qualquer um dos módulos do controlador.

5. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

   Você deve responder com "'y'" quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

6. Atualize o firmware da ponte.

   A partir do ONTAP 9.16,1, você pode usar credenciais para atualizar o firmware da bridge se for necessário pelo servidor para baixar o pacote de firmware.

Se as credenciais não forem necessárias:

a. Atualize o firmware da ponte:

```
system bridge firmware update -bridge <name> -uri <URL-of-firmware-
package>
```

Exemplo

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD
```

Se forem necessárias credenciais:

a. Atualize o firmware da ponte e especifique o nome de usuário necessário:

```
system bridge firmware update -bridge <name> -uri <URL-of-
firmware-package> -username <name>
```

b. Digite a senha quando solicitado na saída, como mostrado no exemplo a seguir:

Exemplo

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD -username abc

(system bridge)

Enter the password:

[Job 70] Job is queued: System bridge firmware update job.
```

7. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

8. Verifique se a atualização do firmware está concluída:

   ```
   job show -name "<job_name>"
   ```

   O exemplo a seguir mostra que a tarefa "atualização do firmware da ponte ystem" ainda está em execução:

```
cluster_A> job show -name "system bridge firmware update"
Owning

Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
2246   job-name
                            cluster_A
                                       node_A_1
                                                      Running
Description: System bridge firmware update job
```

Após cerca de 10 minutos, o novo firmware é totalmente instalado e o estado da tarefa será bem-sucedido:

```
cluster_A> job show -name "system bridge firmware update"

                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
2246   System bridge firmware update
                            cluster_A
                                       node_A_1
                                                      Success
Description: System bridge firmware update job
```

9. Conclua as etapas de acordo com se o gerenciamento na banda está habilitado e qual versão do ONTAP seu sistema está executando:
   - Se você estiver executando o ONTAP 9.4, o gerenciamento na banda não é suportado e o comando deve ser emitido a partir do console de bridge:
     i. Execute o `flashimages` comando no console da ponte e confirme se as versões corretas do firmware são exibidas.

     > O exemplo mostra que a imagem flash principal mostra a nova imagem de firmware, enquanto a imagem flash secundária mostra a imagem antiga.

     ```
     flashimages

      ;Type Version
     ;=====================================================
     Primary 3.16 001H
     Secondary 3.15 002S
     Ready.
     ```

a. Reinicie a ponte executando o `firmwarerestart` comando a partir da ponte.

   - Se você estiver executando o ONTAP 9.5 ou posterior, o gerenciamento na banda é suportado e o comando pode ser emitido a partir do prompt do cluster:

b. Executar o `system bridge run-cli -name <bridge_name> -command FlashImages` comando.

   O exemplo mostra que a imagem flash principal mostra a nova imagem de firmware, enquanto a imagem flash secundária mostra a imagem antiga.

```
cluster_A> system bridge run-cli -name ATTO_7500N_IB_1 -command
FlashImages

[Job 2257]

;Type         Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.


[Job 2257] Job succeeded.
```

a. Se necessário, reinicie a ponte:

```
system bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart
```

A partir da versão 2,95 do firmware ATTO, a ponte será reiniciada automaticamente e esta etapa não é necessária.

10. Verifique se a ponte foi reiniciada corretamente:

```
sysconfig
```

O sistema deve ser cabeado para ter alta disponibilidade de multipath (ambas as controladoras têm acesso por meio das pontes aos compartimentos de disco em cada stack).

```
cluster_A> node run -node cluster_A-01 -command sysconfig
NetApp Release 9.6P8: Sat May 23 16:20:55 EDT 2020
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-
02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

11. Verifique se o firmware do FibreBridge foi atualizado:

    `system bridge show -fields fw-version,symbolic-name`

    ```
    cluster_A> system bridge show -fields fw-version,symbolic-name
    name fw-version symbolic-name
    ---------------- ---------------- -------------
    ATTO_20000010affeaffe 3.10 A06X bridge_A_1a
    ATTO_20000010affeffae 3.10 A06X bridge_A_1b
    ATTO_20000010affeafff 3.10 A06X bridge_A_2a
    ATTO_20000010affeaffa 3.10 A06X bridge_A_2b
    4 entries were displayed.
    ```

12. Verifique se as partições são atualizadas a partir do prompt da ponte:

    `flashimages`

    A imagem flash principal apresenta a nova imagem de firmware, enquanto a imagem flash secundária apresenta a imagem antiga.

    ```
    Ready.
    flashimages

    ;Type         Version
    ;=====================================================
       Primary    3.16 001H
     Secondary    3.15 002S

     Ready.
    ```

13. Repita os passos 5 a 10 para garantir que ambas as imagens flash são atualizadas para a mesma versão.
14. Verifique se ambas as imagens flash estão atualizadas para a mesma versão.

    `flashimages`

    A saída deve mostrar a mesma versão para ambas as partições.

```
Ready.
flashimages

;Type          Version
;=================================================
   Primary     3.16 001H
 Secondary     3.16 001H

 Ready.
```

15. Repita os passos 5 a 13 na próxima ponte até que todas as pontes na configuração do MetroCluster tenham sido atualizadas.

Substituição de uma única ponte FC para SAS

Você pode substituir sem interrupções uma ponte por uma mesma ponte modelo ou por uma nova ponte modelo.

Antes de começar

Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

Sobre esta tarefa

Esse procedimento não causa interrupções e leva aproximadamente 60 minutos para ser concluído.

Este procedimento usa a CLI de bridge para configurar e gerenciar uma bridge e atualizar o firmware da bridge e o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet da bridge. Você pode usar outras interfaces se elas atenderem aos requisitos.

"Requisitos para usar outras interfaces para configurar e gerenciar bridges do FibreBridge"

Informações relacionadas

"Substituição de um par de pontes FibreBridge 6500N por pontes 7600N ou 7500N"

Verificando a conetividade de armazenamento

Antes de substituir bridges, você deve verificar a conetividade de bridge e armazenamento. Familiarizar-se com a saída do comando permite confirmar a conetividade depois de fazer alterações na configuração.

Sobre esta tarefa

Você pode emitir esses comandos a partir do prompt de administrador de qualquer um dos módulos do controlador na configuração do MetroCluster no site em manutenção.

Passos

1. Confirme a conetividade com os discos inserindo o seguinte comando em qualquer um dos nós MetroCluster:

   ```
   run local sysconfig -v
   ```

   A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
```

```
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Troca a quente de uma ponte com uma ponte de substituição do mesmo modelo

Você pode trocar a quente uma ponte com falha por outra ponte do mesmo modelo.

Sobre esta tarefa

Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Se a ponte antiga estiver acessível, você poderá recuperar as informações de configuração.

Se…	Então…
Você está usando gerenciamento de IP	Conete-se à ponte antiga com uma conexão Telnet e copie a saída da configuração da ponte.
Você está usando gerenciamento na banda	Use a CLI do ONTAP para recuperar as informações de configuração com os seguintes comandos: `storage bridge run-cli -name` *`bridge-name`* `-command "info"` `storage bridge run-cli -name` *`bridge-name`* `-command "sasportlist"`

   a. Introduza o comando:

   `storage bridge run-cli -name bridge_A1 -command "info"`

```
info

Device Status          = Good
Unsaved Changes        = None
```

```
Device                 = "FibreBridge 7500N"
Serial Number          = FB7500N100000
Device Version         = 3.10
Board Revision         = 7
Build Number           = 007A
Build Type             = Release
Build Date             = "Aug 20 2019" 11:01:24
Flash Revision         = 0.02
Firmware Version       = 3.10
BCE Version (FPGA 1)   = 15
BAU Version (FPGA 2)   = 33
User-defined name      = "bridgeA1"
World Wide Name        = 20 00 00 10 86 A1 C7 00
MB of RAM Installed    = 512
FC1 Node Name          = 20 00 00 10 86 A1 C7 00
FC1 Port Name          = 21 00 00 10 86 A1 C7 00
FC1 Data Rate          = 16Gb
FC1 Connection Mode    = ptp
FC1 FW Revision        = 11.4.337.0
FC2 Node Name          = 20 00 00 10 86 A1 C7 00
FC2 Port Name          = 22 00 00 10 86 A1 C7 00
FC2 Data Rate          = 16Gb
FC2 Connection Mode    = ptp
FC2 FW Revision        = 11.4.337.0
SAS FW Revision        = 3.09.52
MP1 IP Address         = 10.10.10.10
MP1 IP Subnet Mask     = 255.255.255.0
MP1 IP Gateway         = 10.10.10.1
MP1 IP DHCP            = disabled
MP1 MAC Address        = 00-10-86-A1-C7-00
MP2 IP Address         = 0.0.0.0 (disabled)
MP2 IP Subnet Mask     = 0.0.0.0
MP2 IP Gateway         = 0.0.0.0
MP2 IP DHCP            = enabled
MP2 MAC Address        = 00-10-86-A1-C7-01
SNMP                   = enabled
SNMP Community String  = public
PS A Status            = Up
PS B Status            = Up
Active Configuration   = NetApp

Ready.
```

b. Introduza o comando:

```
storage bridge run-cli -name bridge_A1 -command "sasportlist"
```

```
SASPortList

;Connector      PHY     Link            Speed   SAS Address
;============================================================
Device  A       1       Up              6Gb     5001086000a1c700
Device  A       2       Up              6Gb     5001086000a1c700
Device  A       3       Up              6Gb     5001086000a1c700
Device  A       4       Up              6Gb     5001086000a1c700
Device  B       1       Disabled        12Gb    5001086000a1c704
Device  B       2       Disabled        12Gb    5001086000a1c704
Device  B       3       Disabled        12Gb    5001086000a1c704
Device  B       4       Disabled        12Gb    5001086000a1c704
Device  C       1       Disabled        12Gb    5001086000a1c708
Device  C       2       Disabled        12Gb    5001086000a1c708
Device  C       3       Disabled        12Gb    5001086000a1c708
Device  C       4       Disabled        12Gb    5001086000a1c708
Device  D       1       Disabled        12Gb    5001086000a1c70c
Device  D       2       Disabled        12Gb    5001086000a1c70c
Device  D       3       Disabled        12Gb    5001086000a1c70c
Device  D       4       Disabled        12Gb    5001086000a1c70c
```

2. Se a ponte estiver em uma configuração de MetroCluster conetada à malha, desative todas as portas do switch que se conetam à ou às portas FC da ponte.
3. No prompt do cluster do ONTAP, remova a ponte que está sendo submetida a manutenção do monitoramento de integridade:
   a. Retire a ponte
      `storage bridge remove -name bridge-name`
   b. Veja a lista de pontes monitoradas e confirme que a ponte removida não está presente
      `storage bridge show`
4. Aterre-se corretamente.
5. Desligue a ponte ATTO e retire os cabos de alimentação ligados à ponte.
6. Desligue os cabos que estão ligados à ponte antiga.

   Você deve anotar a porta à qual cada cabo foi conetado.
7. Retire a ponte antiga do rack.
8. Instale a nova ponte no rack.
9. Reconecte o cabo de alimentação e, se estiver configurando para acesso IP à ponte, um cabo Ethernet blindado.

   Não é possível reconetar os cabos SAS ou FC no momento.
10. Ligue a ponte a uma fonte de alimentação e, em seguida, ligue-a.

    O LED bridge Ready pode demorar até 30 segundos a acender, indicando que a ponte concluiu a

sequência de autoteste de ativação.

11. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

    A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.

12. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual* para o modelo de bridge.

    Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

    Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

13. Configure a ponte.

    Se você recuperou as informações de configuração da ponte antiga, use as informações para configurar a nova ponte.

    Certifique-se de anotar o nome de utilizador e a palavra-passe que designou.

    O *ATTO FibreBridge Installation and Operation Manual* para o seu modelo de bridge tem as informações mais atuais sobre os comandos disponíveis e como usá-los.

    > Não configure a sincronização de tempo no ATTO FibreBridge 7600N ou 7500N. A sincronização de tempo para O ATTO FibreBridge 7600N ou 7500N é definida para a hora do cluster depois que a ponte é descoberta pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

    a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

       Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

       Se estiver usando a CLI, você deve executar os seguintes comandos:

       ```
       set ipaddress mp1 _ip-address

       set ipsubnetmask mp1 subnet-mask

       set ipgateway mp1 x.x.x.x

       set ipdhcp mp1 disabled

       set ethernetspeed mp1 1000
       ```

    b. Configure o nome da ponte.

As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set bridgename bridgename
```

c. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte:

```
set SNMP enabled
```

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

14. Configurar as portas FC de ponte.

a. Configure a taxa/velocidade de dados das portas FC em ponte.

A taxa de dados FC suportada depende da ponte do modelo.

- A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
- A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.

> A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pelo switch ao qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCDataRate port-number port-speed
```

b. Se você estiver configurando um FibreBridge 7500N, configure o modo de conexão que a porta usa para "ptp".

> A configuração FCConnMode não é necessária ao configurar uma ponte FibreBridge 7600N.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCConnMode port-number ptp
```

c. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, você deve configurar ou desativar a porta FC2.

- Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.

- Se você não estiver usando a segunda porta, então você deve desativar a porta:

  `FCPortDisable port-number`

d. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, desative as portas SAS não utilizadas:

   `SASPortDisable sas-port`

   > As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas. Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas.

15. Proteja o acesso à ponte e salve a configuração da ponte.

a. No prompt do controlador, verifique o status das pontes: `storage bridge show`

   A saída mostra qual ponte não está protegida.

b. Verifique o estado das portas da ponte não protegida:

   `info`

   A saída mostra o status das portas Ethernet MP1 e MP2.

c. Se a porta Ethernet MP1 estiver ativada, execute o seguinte comando:

   `set EthernetPort mp1 disabled`

   > Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2.

d. Salve a configuração da ponte.

   Você deve executar os seguintes comandos:

   `SaveConfiguration`

   `FirmwareRestart`

Você é solicitado a reiniciar a ponte.

16. Conete os cabos FC às mesmas portas da nova ponte.
17. Atualize o firmware do FibreBridge em cada ponte.

    Se a nova ponte for do mesmo tipo que a ponte parceira, atualize para o mesmo firmware que a ponte parceira. Se a nova ponte for um tipo diferente da ponte do parceiro, atualize para o firmware mais recente suportado pela ponte e versão do ONTAP. Consulte "Atualizando o firmware em uma ponte FibreBridge"

18. reconecte os cabos SAS às mesmas portas da nova ponte.

    Você deve substituir os cabos que conetam a ponte à parte superior ou inferior da pilha da prateleira. As pontes FibreBridge 7600N e 7500N requerem cabos mini-SAS para essas conexões.

Aguarde pelo menos 10 segundos antes de ligar a porta. Os conetores de cabo SAS são chaveados; quando orientados corretamente para uma porta SAS, o conetor se encaixa no lugar e o LED LNK da porta SAS do compartimento de disco fica verde. Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor). Para controladores, a orientação das portas SAS pode variar dependendo do modelo da plataforma; portanto, a orientação correta do conetor do cabo SAS varia.

19. Verifique se cada bridge pode ver todas as unidades de disco e prateleiras de disco às quais a ponte está conetada.

Se você estiver usando o…	Então…
ATTO ExpressNAV GUI	a. Em um navegador da Web compatível, insira o endereço IP da ponte na caixa do navegador. Você é levado para a página inicial DO ATTO FibreBridge, que tem um link. b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte. A página de status ATTO FibreBridge aparece com um menu à esquerda. c. Clique em **Avançado** no menu. d. Ver os dispositivos ligados: `sastargets` e. Clique em **Enviar**.
Conexão de porta serial	Ver os dispositivos ligados: `sastargets`

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos.

Se a resposta de texto truncada aparecer no início da saída, você pode usar o Telnet para se conetar à ponte e, em seguida, exibir toda a saída usando o `sastargets` comando.

A saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID         Type SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK 3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK 3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK 3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK 3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK 3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK 3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK 3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK 3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK 3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK 3QP1FXW600009940VERQ
```

20. Verifique se a saída do comando mostra que a ponte está conetada a todos os discos e compartimentos de disco apropriados na pilha.

Se a saída for…	Então…
Correto	Repita Passo 19 para cada ponte restante.
Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo Passo 18. b. Repita Passo 19.

21. Se a ponte estiver em uma configuração de MetroCluster conetada à malha, reative a porta do switch FC desativada no início deste procedimento.

    Este deve ser o porto que se coneta à ponte.

22. No console do sistema de ambos os módulos do controlador, verifique se todos os módulos do controlador têm acesso através da nova ponte para as prateleiras de disco (ou seja, se o sistema está cabeado para Multipath HA):

    ```
    run local sysconfig
    ```

    Pode levar até um minuto para o sistema concluir a descoberta.

    Se a saída não indicar Multipath HA, você deve corrigir o cabeamento SAS e FC porque nem todas as unidades de disco estão acessíveis por meio da nova ponte.

    A saída a seguir indica que o sistema é cabeado para Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

Quando o sistema não é cabeado como Multipath HA, reiniciar uma ponte pode causar perda de acesso às unidades de disco e resultar em pânico de vários discos.

23. Se estiver executando o ONTAP 9.4 ou anterior, verifique se a ponte está configurada para SNMP.

    Se você estiver usando a CLI de bridge, execute o seguinte comando:

    ```
    get snmp
    ```

24. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

    a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
9,5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9,4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    b. Verifique se a ponte foi adicionada e está configurada corretamente:

    `storage bridge show`

    Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de saúde do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

    O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

25. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed
    `node run -node node-name sysconfig -a`
    b. Verifique se há alertas de integridade em ambos os clusters
    `system health alert show`
    c. Confirme a configuração do MetroCluster e se o modo operacional está normal
    `metrocluster show`
    d. Execute uma verificação MetroCluster
    `metrocluster check run`
    e. Exibir os resultados da verificação MetroCluster
    `metrocluster check show`
    f. Verifique se existem alertas de estado nos interrutores (se presentes)
    `storage switch show`
    g. Execute o Config Advisor.

    "NetApp Downloads: Config Advisor"

    h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Informações relacionadas

"Gerenciamento na banda das pontes FC para SAS"

Troca quente de uma FibreBridge 7500N com uma ponte 7600N

Você pode trocar uma ponte FibreBridge 7500N por uma ponte 7600N.

Sobre esta tarefa

Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Se a ponte estiver em uma configuração de MetroCluster conetada à malha, desative todas as portas do switch que se conetam à ou às portas FC da ponte.
2. No prompt do cluster do ONTAP, remova a ponte que está sendo submetida a manutenção do monitoramento de integridade:
   a. Retire a ponte
      `storage bridge remove -name bridge-name`
   b. Veja a lista de pontes monitoradas e confirme que a ponte removida não está presente
      `storage bridge show`
3. Aterre-se corretamente.
4. Retire os cabos de alimentação ligados à ponte para desligar a ponte.
5. Desligue os cabos que estão ligados à ponte antiga.

   Você deve anotar a porta à qual cada cabo foi conetado.
6. Retire a ponte antiga do rack.
7. Instale a nova ponte no rack.
8. Volte a ligar o cabo de alimentação e o cabo Ethernet blindado.

   > Não é possível reconetar os cabos SAS ou FC no momento.
9. Ligue a ponte a uma fonte de alimentação e, em seguida, ligue-a.

   O LED bridge Ready pode demorar até 30 segundos a acender, indicando que a ponte concluiu a sequência de autoteste de ativação.
10. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

    A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.
11. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

    A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.
12. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual*

para o modelo de bridge.

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

13. Configure as bridges.

    Certifique-se de anotar o nome de utilizador e a palavra-passe que designou.

    O *ATTO FibreBridge Installation and Operation Manual* para o seu modelo de bridge tem as informações mais atuais sobre os comandos disponíveis e como usá-los.

    > Não configure a sincronização de tempo no FibreBridge 7600N. A sincronização de tempo para o FibreBridge 7600N é definida para a hora do cluster após a descoberta da ponte pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

    a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

       Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

       Se estiver usando a CLI, você deve executar os seguintes comandos:

       ```
       set ipaddress mp1 ip-address

       set ipsubnetmask mp1 subnet-mask

       set ipgateway mp1 x.x.x.x

       set ipdhcp mp1 disabled

       set ethernetspeed mp1 1000
       ```

    b. Configure o nome da ponte.

       As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

       Exemplos de nomes de bridge para um grupo de pilha em cada local:

       - bridge_A_1a
       - bridge_A_1b
       - bridge_B_1a
       - bridge_B_1b

         Se estiver usando a CLI, você deve executar o seguinte comando:

```
set bridgename bridgename
```

a. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte
`set SNMP enabled`

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

14. Configurar as portas FC de ponte.

a. Configure a taxa/velocidade de dados das portas FC em ponte.

A taxa de dados FC suportada depende da ponte do modelo.

- A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
- A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.

> A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pela porta FC do módulo ou switch do controlador ao qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCDataRate port-number port-speed
```

b. Tem de configurar ou desativar a porta FC2.

- Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.
- Se você não estiver usando a segunda porta, então você deve desativar a porta não utilizada:

```
FCPortDisable port-number
```

O exemplo a seguir mostra a desativação da porta FC 2:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

c. Desative as portas SAS não utilizadas:

```
SASPortDisable sas-port
```

> As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas.

Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas. O exemplo a seguir mostra a desativação da porta SAS B. você deve desabilitar as portas SAS C e D da mesma forma:

```
SASPortDisable b

SAS Port B has been disabled.
```

15. Proteja o acesso à ponte e salve a configuração da ponte.

    a. No prompt do controlador, verifique o status das pontes:

       `storage bridge show`

       A saída mostra qual ponte não está protegida.

    b. Verifique o estado das portas da ponte não protegida:

       `info`

       A saída mostra o status das portas Ethernet MP1 e MP2.

    c. Se a porta Ethernet MP1 estiver ativada, execute o seguinte comando:

       `set EthernetPort mp1 disabled`

       Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2.

    d. Salve a configuração da ponte.

       Você deve executar os seguintes comandos

       `SaveConfiguration`

       `FirmwareRestart`

    Você é solicitado a reiniciar a ponte.

16. Conete os cabos FC às mesmas portas da nova ponte.
17. Atualize o firmware do FibreBridge em cada ponte.

    "Atualize o firmware em uma ponte FibreBridge"

18. reconecte os cabos SAS às mesmas portas da nova ponte.

    Aguarde pelo menos 10 segundos antes de ligar a porta. Os conetores de cabo SAS são chaveados; quando orientados corretamente para uma porta SAS, o conetor se encaixa no lugar e o LED LNK da porta SAS do compartimento de disco fica verde. Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor). Para controladores, a orientação das portas SAS pode variar dependendo do modelo da plataforma; portanto, a orientação correta do conetor do cabo SAS varia.

19. Verifique se cada bridge pode ver todas as unidades de disco e compartimentos de disco aos quais a

ponte está conetada:

```
sastargets
```

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos.

A saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

20. Verifique se a saída do comando mostra que a ponte está conetada a todos os discos e compartimentos de disco apropriados na pilha.

Se a saída for…	Então…
Correto	Repita o passo anterior para cada ponte restante.
Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo Passo 18. b. Repita o passo anterior.

21. Se a ponte estiver em uma configuração de MetroCluster conetada à malha, reative a porta do switch FC desativada no início deste procedimento.

    Este deve ser o porto que se coneta à ponte.

22. No console do sistema de ambos os módulos do controlador, verifique se todos os módulos do controlador têm acesso através da nova ponte para as prateleiras de disco (ou seja, se o sistema está cabeado para Multipath HA):

    ```
    run local sysconfig
    ```

    Pode levar até um minuto para o sistema concluir a descoberta.

    Se a saída não indicar Multipath HA, você deve corrigir o cabeamento SAS e FC porque nem todas as unidades de disco estão acessíveis por meio da nova ponte.

    A saída a seguir indica que o sistema é cabeado para Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

Quando o sistema não é cabeado como Multipath HA, reiniciar uma ponte pode causar perda de acesso às unidades de disco e resultar em pânico de vários discos.

23. Se estiver executando o ONTAP 9.4 ou anterior, verifique se a ponte está configurada para SNMP.

    Se você estiver usando a CLI de bridge, execute o seguinte comando:

    `get snmp`

24. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

    a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
9,5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9,4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    b. Verifique se a ponte foi adicionada e está configurada corretamente:

    `storage bridge show`

    Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de saúde do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

    O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge               Symbolic Name Is Monitored  Monitor Status  Vendor
Model                 Bridge WWN
------------------  ------------ -----------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

25. Verifique a operação da configuração do MetroCluster no ONTAP:

    a. Verifique se o sistema é multipathed
    `node run -node node-name sysconfig -a`

    b. Verifique se há alertas de integridade em ambos os clusters
    `system health alert show`

    c. Confirme a configuração do MetroCluster e se o modo operacional está normal
    `metrocluster show`

    d. Execute uma verificação MetroCluster
    `metrocluster check run`

    e. Exibir os resultados da verificação MetroCluster

    ```
    metrocluster check show
    ```

    f. Verifique se existem alertas de estado nos interrutores (se presentes)
    `storage switch show`

    g. Execute o Config Advisor.

    "NetApp Downloads: Config Advisor"

    h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Informações relacionadas

"Gerenciamento na banda das pontes FC para SAS"

Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N

Você pode trocar uma ponte FibreBridge 6500N por uma ponte FibreBridge 7600N ou 7500N para substituir uma ponte com falha ou atualizar sua ponte em uma configuração MetroCluster conetada à malha ou conetada à ponte.

Sobre esta tarefa

- Este procedimento é para troca automática de uma única ponte FibreBridge 6500N com uma única ponte FibreBridge 7600N ou 7500N.
- Quando você troca a quente uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N, você deve usar apenas uma porta FC e uma porta SAS na ponte FibreBridge 7600N ou 7500N.
- Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

> Se você estiver trocando as duas pontes FibreBridge 6500N em um par, você deve usar o "Consolide várias pilhas de storage" procedimento para instruções de zoneamento. Ao substituir ambas as pontes FibreBridge 6500N na ponte, você pode aproveitar os portos adicionais na ponte FibreBridge 7600N ou 7500N.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Execute um dos seguintes procedimentos:
   - Se a ponte com falha estiver em uma configuração MetroCluster conetada à malha, desative a porta do switch que se coneta à porta FC da ponte.
   - Se a ponte com falha estiver em uma configuração Stretch MetroCluster, use uma das portas FC disponíveis.
2. No prompt do cluster do ONTAP, remova a ponte que está sendo submetida a manutenção do monitoramento de integridade:
   a. Retire a ponte:

      `storage bridge remove -name` *`bridge-name`*

   b. Veja a lista de pontes monitoradas e confirme se a ponte removida não está presente:

      `storage bridge show`

3. Aterre-se corretamente.
4. Desligue o interrutor de alimentação da ponte.
5. Desconete os cabos conetados da prateleira às portas de ponte e cabos de alimentação do FibreBridge 6500N.

   Você deve anotar as portas às quais cada cabo foi conetado.

6. Remova a ponte FibreBridge 6500N que você precisa substituir do rack.
7. Instale a nova ponte FibreBridge 7600N ou 7500N no rack.

8. Volte a ligar o cabo de alimentação e, se necessário, o cabo Ethernet blindado.

   Não reconecte os cabos SAS ou FC neste momento.

9. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

   A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.

10. Se estiver configurando para gerenciamento IP, conete a porta 1 de gerenciamento Ethernet em cada bridge à rede usando um cabo Ethernet.

    Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

    A porta 1 de gerenciamento Ethernet permite que você baixe rapidamente o firmware da ponte (usando interfaces de gerenciamento ATTO ExpressNAV ou FTP) e recupere arquivos principais e extraia logs.

11. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual* para o modelo de bridge.

    Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

    Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

12. Configure a ponte.

    Se você recuperou as informações de configuração da ponte antiga, use as informações para configurar a nova ponte.

    Certifique-se de anotar o nome de utilizador e a palavra-passe que designou.

    O *ATTO FibreBridge Installation and Operation Manual* para o seu modelo de bridge tem as informações mais atuais sobre os comandos disponíveis e como usá-los.

    Não configure a sincronização de tempo no ATTO FibreBridge 7600N ou 7500N. A sincronização de tempo para O ATTO FibreBridge 7600N ou 7500N é definida para a hora do cluster depois que a ponte é descoberta pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

    a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

       Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

       Se estiver usando a CLI, você deve executar os seguintes comandos:

```
set ipaddress mp1 ip-address

set ipsubnetmask mp1 subnet-mask

set ipgateway mp1 x.x.x.x

set ipdhcp mp1 disabled

set ethernetspeed mp1 1000
```

b. Configure o nome da ponte.

As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

Exemplos de nomes de bridge para um grupo de pilha em cada local:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set bridgename bridgename
```

a. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte
`set SNMP enabled`

Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

13. Configurar as portas FC de ponte.

a. Configure a taxa/velocidade de dados das portas FC em ponte.

A taxa de dados FC suportada depende da ponte do modelo.

- A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
- A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.
- A ponte FibreBridge 6500N suporta até 8, 4 ou 2 Gbps.

A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pelo switch ao qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCDataRate port-number port-speed
```

b. Se você estiver configurando uma ponte FibreBridge 7500N ou 6500N, configure o modo de conexão que a porta usa para ptp.

A configuração FCConnMode não é necessária ao configurar uma ponte FibreBridge 7600N.

Se estiver usando a CLI, você deve executar o seguinte comando:

```
set FCConnMode port-number ptp
```

c. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, você deve configurar ou desativar a porta FC2.
   - Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.
   - Se você não estiver usando a segunda porta, então você deve desativar a porta:

     ```
     FCPortDisable port-number
     ```

d. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, desative as portas SAS não utilizadas:

   ```
   SASPortDisable sas-port
   ```

   As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas. Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas.

14. Proteja o acesso à ponte e salve a configuração da ponte.

    a. No prompt do controlador, verifique o status das pontes:

       ```
       storage bridge show
       ```

       A saída mostra qual ponte não está protegida.

    b. Verifique o estado das portas da ponte não protegida:

       ```
       info
       ```

       A saída mostra o status das portas Ethernet MP1 e MP2.

    c. Se a porta Ethernet MP1 estiver ativada, execute o seguinte comando:

       ```
       set EthernetPort mp1 disabled
       ```

       Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2.

    d. Salve a configuração da ponte.

       Você deve executar os seguintes comandos:

       ```
       SaveConfiguration
       ```

       ```
       FirmwareRestart
       ```

Você é solicitado a reiniciar a ponte.

15. Ative o monitoramento de integridade para a ponte FibreBridge 7600N ou 7500N.
16. Conete os cabos FC às portas Fibre Channel 1 na nova ponte.

    Você deve enviar a porta FC para a mesma porta do switch ou controlador à qual a ponte FibreBridge 6500N foi conetada.

17. Atualize o firmware do FibreBridge em cada ponte.

    Se a nova ponte for do mesmo tipo que a ponte parceira, atualize para o mesmo firmware que a ponte parceira. Se a nova ponte for um tipo diferente da ponte do parceiro, atualize para o firmware e a versão mais recentes do ONTAP suportados pela ponte.

    "Atualize o firmware em uma ponte FibreBridge"

18. Reconete os cabos SAS às portas SAS A na nova ponte.

    A porta SAS deve ser cabeada para a mesma porta de gaveta à qual a ponte FibreBridge 6500N foi conetada.

    > Não force um conetor para uma porta. Os cabos mini-SAS são chaveados; quando orientados corretamente para uma porta SAS, o cabo SAS clica no lugar e o LED LNK da porta SAS da gaveta de disco acende-se a verde. Para prateleiras de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).para controladores, a orientação das portas SAS pode variar dependendo do modelo da plataforma; portanto, a orientação correta do conetor de cabo SAS varia.

19. Verifique se a ponte pode detetar todas as unidades de disco e compartimentos de disco a que está conetada.

Se você estiver usando o…	Então…
ATTO ExpressNAV GUI	a. Em um navegador da Web compatível, insira o endereço IP da ponte na caixa do navegador. Você é levado para a página inicial DO ATTO FibreBridge, que tem um link. b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte. A página de status ATTO FibreBridge aparece com um menu à esquerda. c. Clique em **Avançado** no menu. d. Digite o seguinte comando e clique em **Submit** para ver a lista de discos visíveis para a ponte: `sastargets`

Conexão de porta serial	Exiba a lista de discos visíveis para a ponte: `sastargets`

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos. Por exemplo, a saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

Se o texto "Esponse truncado" aparecer no início da saída, você pode usar o Telnet para acessar a ponte e digitar o mesmo comando para ver toda a saída.

20. Verifique se o comando output mostra que a ponte está conetada a todos os discos e compartimentos de disco necessários na pilha.

Se a saída for…	Então…
Correto	Repita o passo anterior para cada ponte restante.
Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo Passo 18. b. Repita o passo anterior para cada ponte restante.

21. Reative a porta do switch FC que se coneta à ponte.
22. Verifique se todas as controladoras têm acesso por meio da nova ponte aos compartimentos de disco (se o sistema está cabeado para Multipath HA), no console do sistema de ambas as controladoras:

```
run local sysconfig
```

Pode levar até um minuto para o sistema concluir a descoberta.

Por exemplo, a saída a seguir mostra que o sistema está cabeado para Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

Se o comando OUTPUT indicar que a configuração é HA de caminho misto ou de caminho único, você deve corrigir o cabeamento SAS e FC porque nem todas as unidades de disco estão acessíveis por meio da nova ponte.

Quando o sistema não é cabeado como Multipath HA, reiniciar uma ponte pode causar perda de acesso às unidades de disco e resultar em pânico de vários discos.

23. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

    a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
9,5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9,4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    b. Verifique se a ponte foi adicionada e está configurada corretamente
    `storage bridge show`

    Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de saúde do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

    O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

24. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed:

       `node run -node node-name sysconfig -a`

    b. Verifique se há alertas de integridade em ambos os clusters
       `system health alert show`
    c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

       `metrocluster show`

    d. Execute uma verificação MetroCluster:

       `metrocluster check run`

    e. Apresentar os resultados da verificação MetroCluster:

       `metrocluster check show`

    f. Verifique se existem alertas de estado nos interrutores (se presentes):

       `storage switch show`

    g. Execute o Config Advisor.

       "NetApp Downloads: Config Advisor"

    h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

25. Após a substituição da peça, devolva a peça com falha à NetApp, conforme descrito nas instruções de RMA fornecidas com o kit. Consulte a "Substituição Devolução artigo" página para obter mais informações.

Informações relacionadas

"Gerenciamento na banda das pontes FC para SAS"

Substituição de um par de pontes FibreBridge 6500N por pontes 7600N ou 7500N

Para aproveitar a porta FC2 adicional nas pontes FibreBridge 7600N ou 7500N e reduzir a utilização de rack, você pode substituir 6500N pontes sem interrupções e consolidar até quatro stacks de storage atrás de um único par de pontes FibreBridge 7600N ou 7500N.

Antes de começar

Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

Sobre esta tarefa

Deve utilizar este procedimento se:

- Você está substituindo um par de pontes FibreBridge 6500N por pontes FibreBridge 7600N ou 7500N.

  Após a substituição, ambas as pontes no par devem ser do mesmo modelo.

- Você substituiu anteriormente uma única ponte FibreBridge 6500N por uma ponte 7600N ou 7500N e agora está substituindo a segunda ponte no par.
- Você tem um par de bridgeBridge 7600N ou 7500N com portas SAS disponíveis e está consolidando stacks de armazenamento SAS que estão atualmente conetadas usando bridgeBridge 6500N.

Esse procedimento não causa interrupções e leva aproximadamente duas horas para ser concluído.

Informações relacionadas

"Substituição de uma única ponte FC para SAS"

Verificando a conetividade de armazenamento

Antes de substituir bridges, você deve verificar a conetividade de bridge e armazenamento. Familiarizar-se com a saída do comando permite confirmar a conetividade depois de fazer alterações na configuração.

Você pode emitir esses comandos a partir do prompt de administrador de qualquer um dos módulos do controlador na configuração do MetroCluster no site em manutenção.

1. Confirme a conetividade com os discos inserindo o seguinte comando em qualquer um dos nós MetroCluster:

   ```
   run local sysconfig -v
   ```

   A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   ```

```
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
```

```
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Ponte FibreBridge 6500N pontes para criar um par de pontes FibreBridge 7600N ou 7500N

Para trocar a quente uma ou duas pontes FibreBridge 6500N para criar uma configuração com um par de pontes FibreBridge 7600N ou 7500N, você deve substituir as pontes uma de cada vez e seguir o procedimento de cabeamento correto. O novo cabeamento é diferente do cabeamento original.

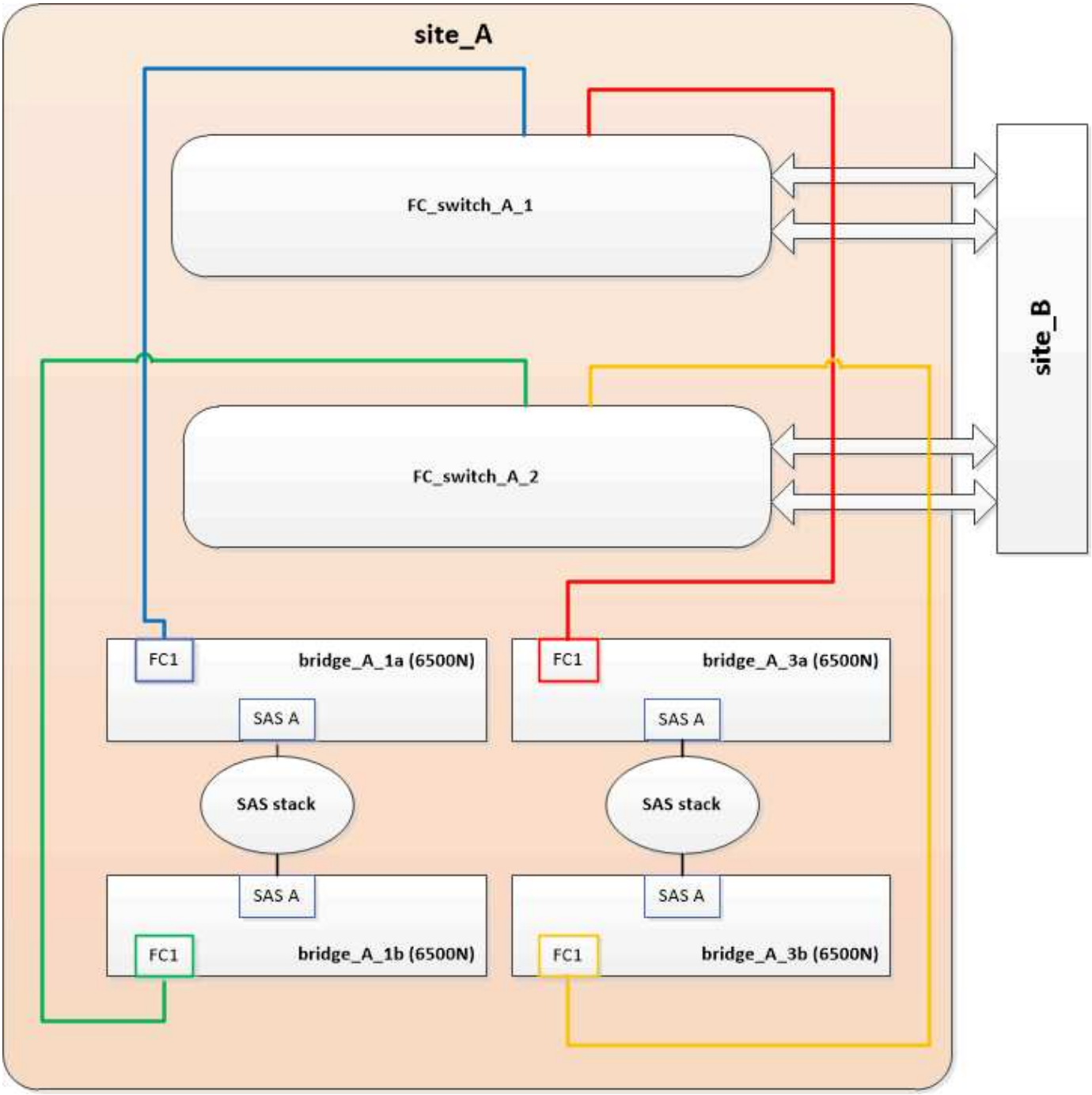
Sobre esta tarefa

Você também pode usar este procedimento se as seguintes condições forem verdadeiras:

- Você está substituindo um par de bridges do FibreBridge 6500N que estão conetadas à mesma pilha de armazenamento SAS.
- Você substituiu anteriormente uma ponte FibreBridge 6500N no par e sua pilha de armazenamento está configurada com uma ponte FibreBridge 6500N e uma ponte FibreBridge 7600N ou 7500N.

  Neste caso, você deve começar com o passo abaixo para trocar a ponte FibreBridge 6500N inferior com uma ponte FibreBridge 7600N ou 7500N.

O diagrama a seguir mostra um exemplo da configuração inicial, na qual quatro bridgeBridge 6500N estão conetando duas stacks de armazenamento SAS:



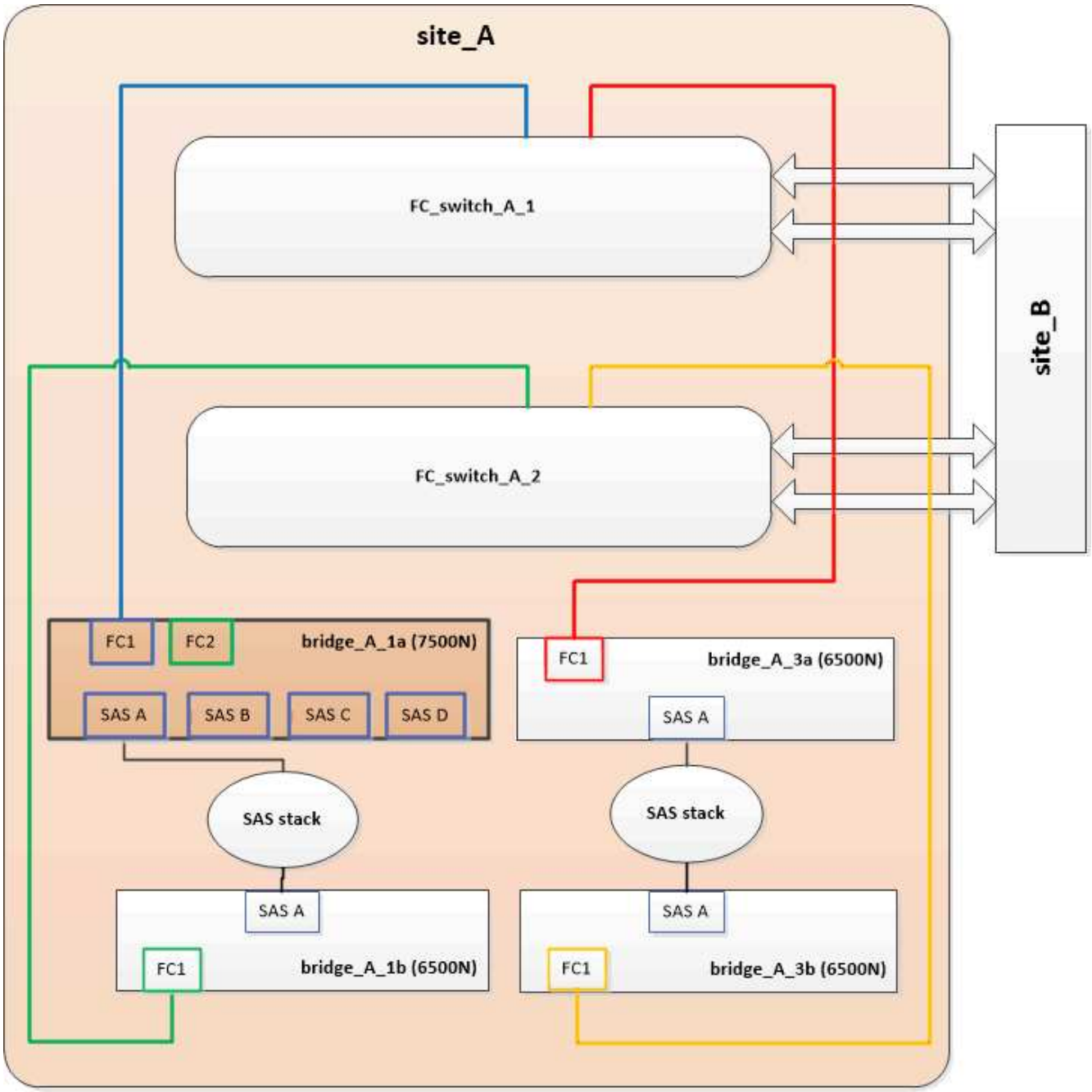
Passos

1. Usando as diretrizes a seguir, troque a ponte FibreBridge 6500N superior por uma ponte FibreBridge 7600N ou 7500N usando o procedimento em "Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N":

   - Ligue a porta FibreBridge 7600N ou 7500N bridge FC1 ao comutador ou controlador.

     Esta é a mesma conexão que foi feita ao porto da ponte FC1 de FibreBridge 6500N.

   - Não conete a porta FibreBridge 7600N ou 7500N bridge FC2 neste momento. O diagrama a seguir mostra que bridge_A_1a foi substituída e agora é uma ponte FibreBridge 7600N ou 7500N:



2. Confirme a conetividade com os discos conetados em ponte e se o novo FibreBridge 7500N está visível na configuração:

```
run local sysconfig -v
```

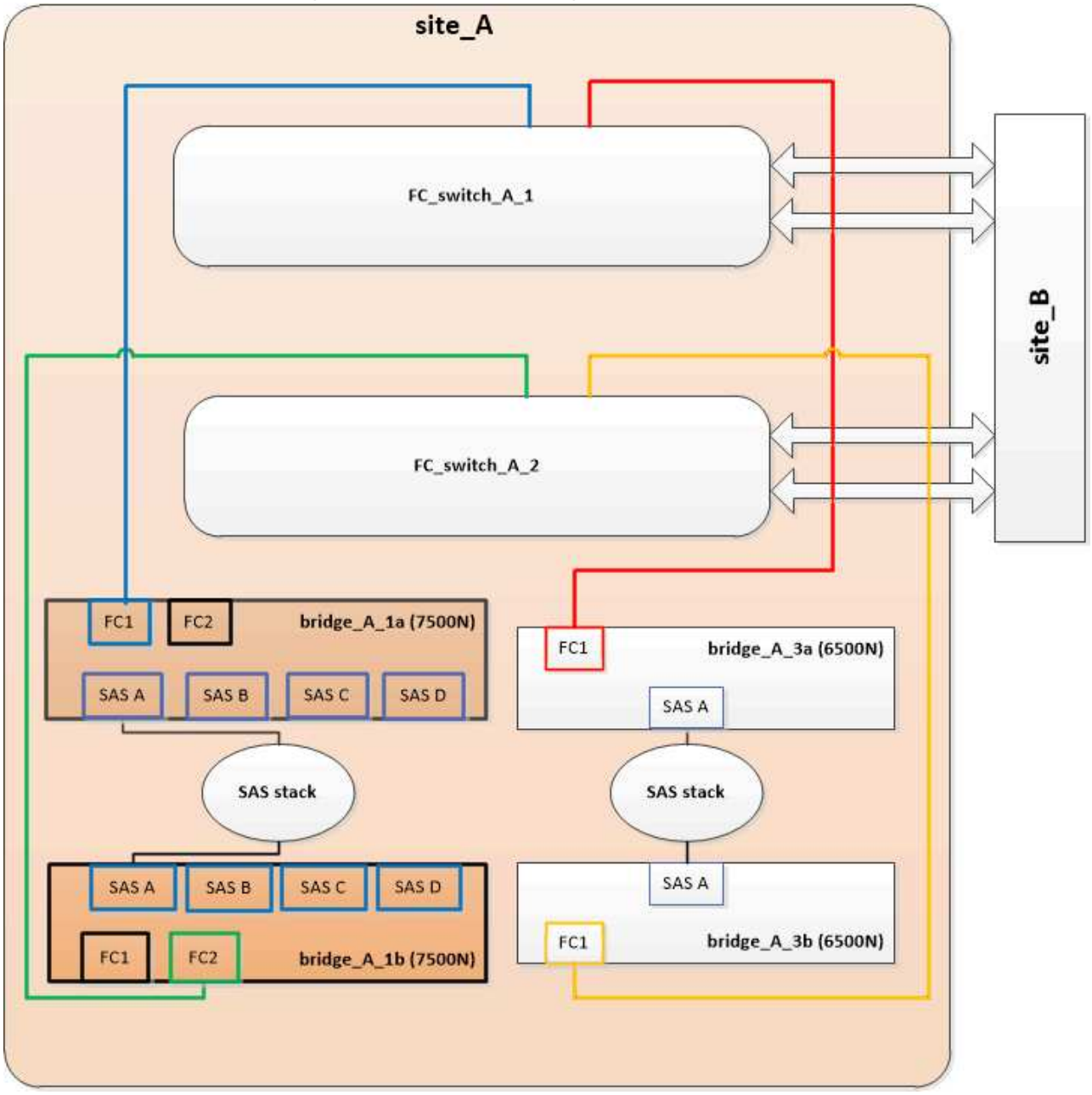
```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
```

```
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104**<===**
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

3. Usando as diretrizes a seguir, troque a ponte FibreBridge 6500N inferior por uma ponte FibreBridge 7600N ou 7500N usando o procedimento em "Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N":
   - Ligue a porta FibreBridge 7600N ou 7500N bridge FC2 ao comutador ou controlador.

     Esta é a mesma conexão que foi feita ao porto da ponte FC1 de FibreBridge 6500N.

   - Não conete a porta FibreBridge 7600N ou 7500N bridge FC1 neste momento.



4. Confirme a conetividade com os discos conetados em ponte:

   ```
   run local sysconfig -v
   ```

   A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
```

.
.
.

Cabeamento das portas SAS da ponte ao consolidar o armazenamento por trás das pontes FibreBridge 7600N ou 7500N

Ao consolidar várias stacks de storage SAS atrás de um único par de pontes FibreBridge 7600N ou 7500N com portas SAS disponíveis, você precisa mover os cabos SAS superior e inferior para as novas pontes.

Sobre esta tarefa

As portas SAS da ponte FibreBridge 6500N usam conetores QSFP. As portas SAS de ponte FibreBridge 7600N ou 7500N usam conetores mini-SAS.

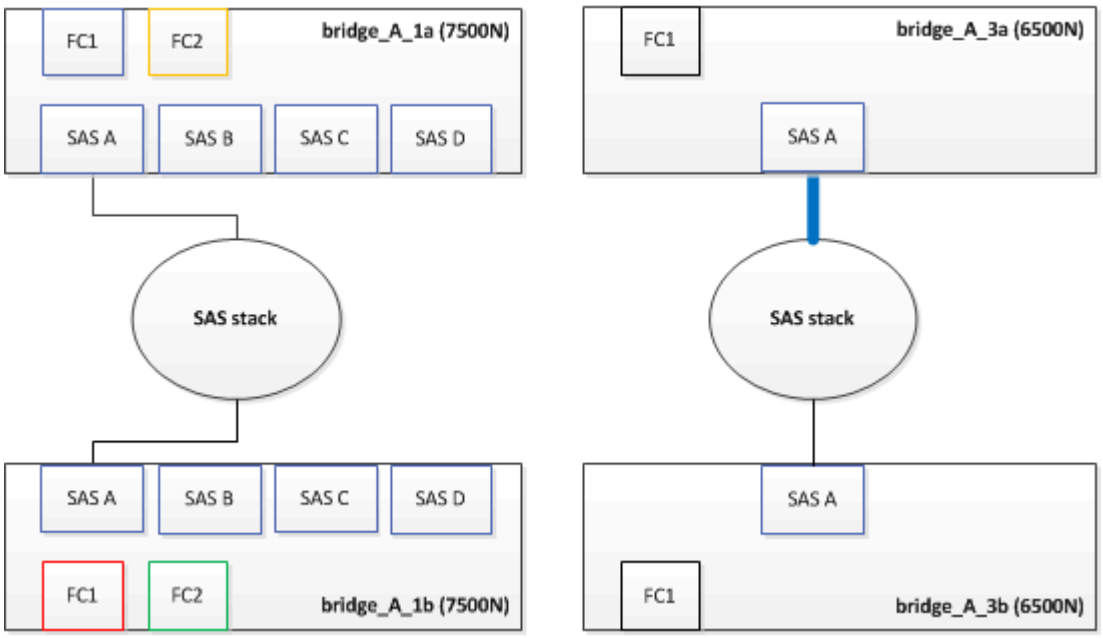
Se você inserir um cabo SAS na porta errada, ao remover o cabo de uma porta SAS, deverá aguardar pelo menos 120 segundos antes de conetar o cabo a uma porta SAS diferente. Se não o fizer, o sistema não reconhecerá que o cabo foi movido para outra porta.

Aguarde pelo menos 10 segundos antes de ligar a porta. Os conetores de cabo SAS são chaveados; quando orientados corretamente para uma porta SAS, o conetor se encaixa no lugar e o LED LNK da porta SAS do compartimento de disco fica verde. Para compartimentos de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conetor).

Passos

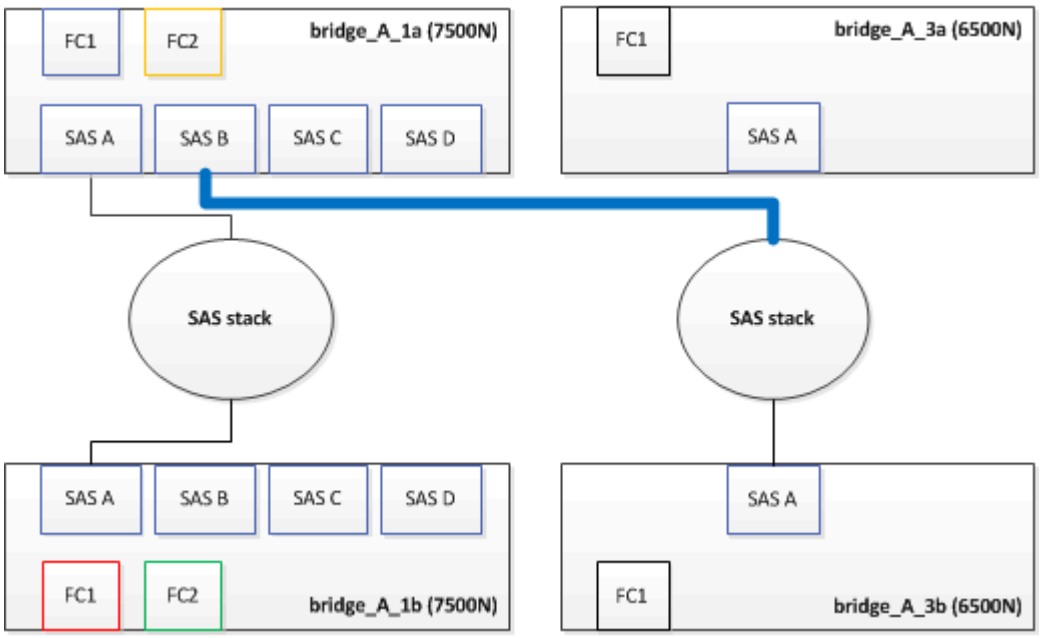
1. Remova o cabo que coneta a porta SAS A da ponte FibreBridge 6500N superior à gaveta SAS superior, certificando-se de anotar a porta SAS na gaveta de armazenamento à qual ela se coneta.

   O cabo é mostrado em azul no exemplo a seguir:



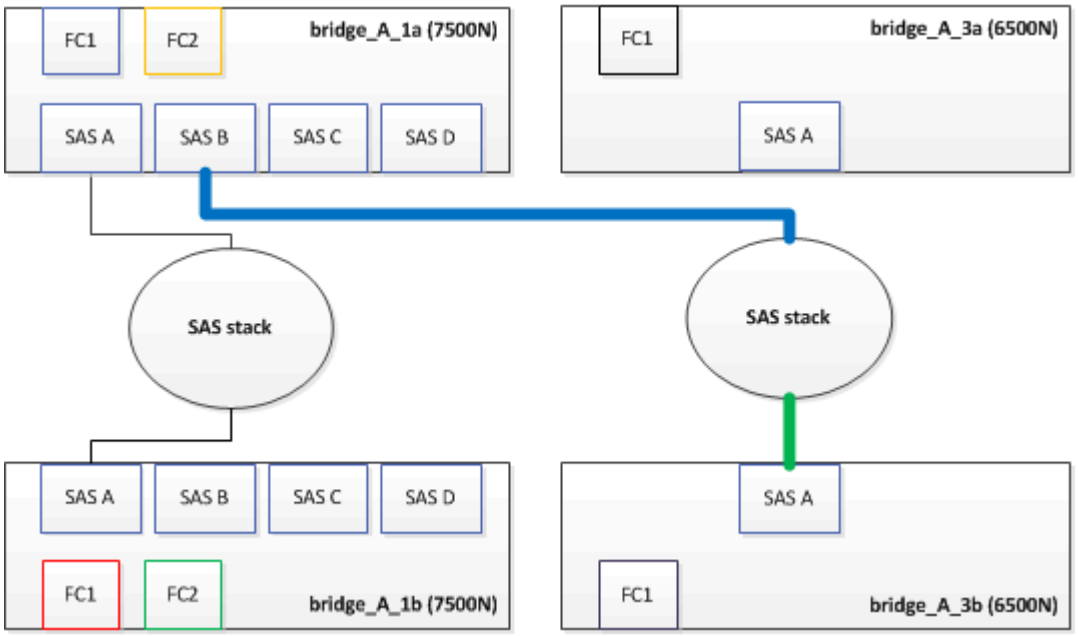
2. Usando um cabo com um conetor mini-SAS, conete a mesma porta SAS no compartimento de armazenamento à porta SAS B da ponte FibreBridge 7600N ou 7500N superior.

O cabo é mostrado em azul no exemplo a seguir:



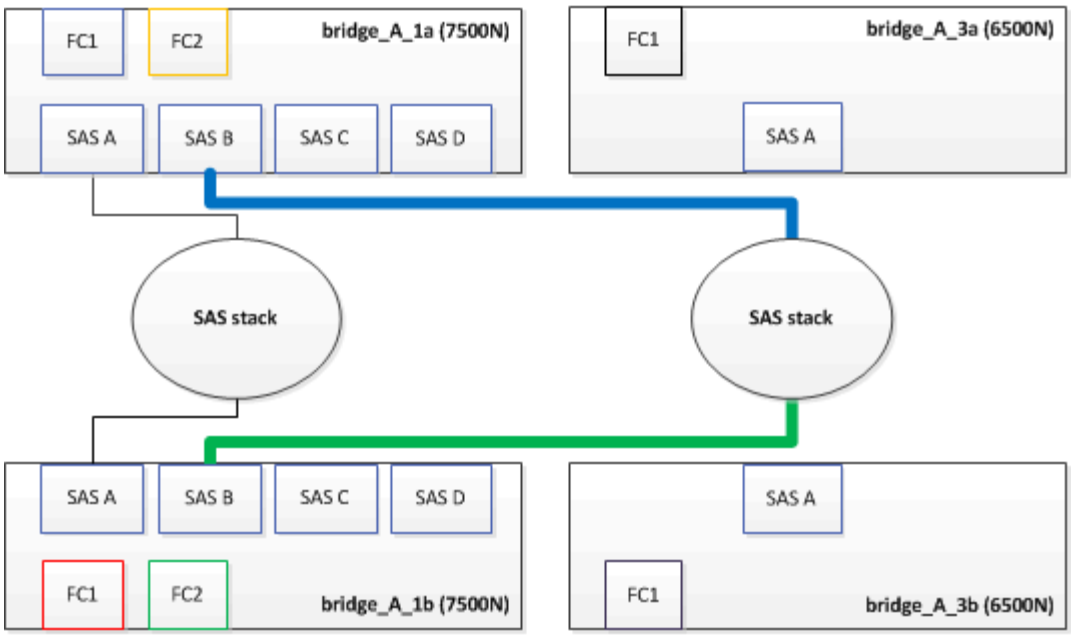
3. Remova o cabo que coneta a porta SAS A da ponte FibreBridge 6500N inferior à gaveta SAS superior, certificando-se de anotar a porta SAS na gaveta de armazenamento à qual ela se coneta.

   Este cabo é apresentado a verde no seguinte exemplo:



4. Usando um cabo com um conetor mini-SAS, conete a mesma porta SAS no compartimento de armazenamento à porta SAS B da ponte FibreBridge 7600N ou 7500N inferior.

   Este cabo é apresentado a verde no seguinte exemplo:



5. Confirme a conetividade com os discos conetados em ponte:

   `run local sysconfig -v`

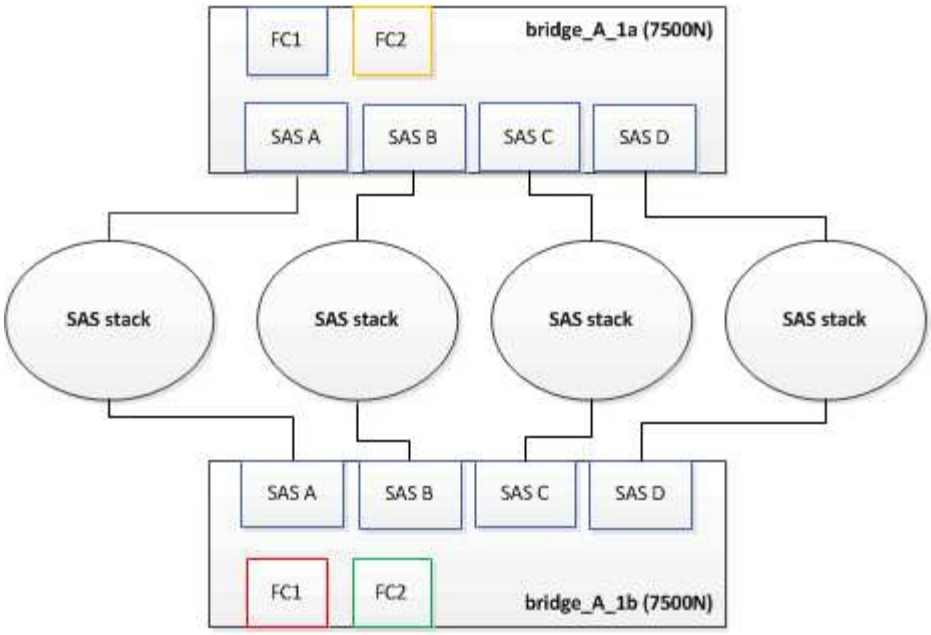
   A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
```

```
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

6. Remova as pontes antigas do FibreBridge 6500N que não estão mais conetadas ao armazenamento SAS.
7. Aguarde dois minutos para que o sistema reconheça as alterações.
8. Se o sistema tiver sido cabeado incorretamente, remova o cabo, corrija o cabeamento e, em seguida, reconete o cabo correto.
9. Se necessário, repita as etapas anteriores para mover até duas stacks SAS adicionais atrás das novas bridges 7600N ou 7500N do FibreBridge, usando as portas SAS C e d..

   Cada pilha SAS deve ser conetada à mesma porta SAS na ponte superior e inferior. Por exemplo, se a conexão superior da pilha estiver conetada à porta SAS B da ponte superior, a conexão inferior deverá ser conetada à porta SAS B da ponte inferior.



Atualizando zoneamento ao adicionar bridgeBridge 7600N ou 7500N bridges a uma configuração

O zoneamento deve ser alterado quando você estiver substituindo as pontes FibreBridge 6500N por pontes FibreBridge 7600N ou 7500N e usando ambas as portas FC nas pontes FibreBridge 7600N ou 7500N. As alterações necessárias dependem se você está executando uma versão do ONTAP anterior a 9,1 ou 9,1 e posterior.

Atualizando o zoneamento ao adicionar bridgeBridge 7500N a uma configuração (antes do ONTAP 9.1)

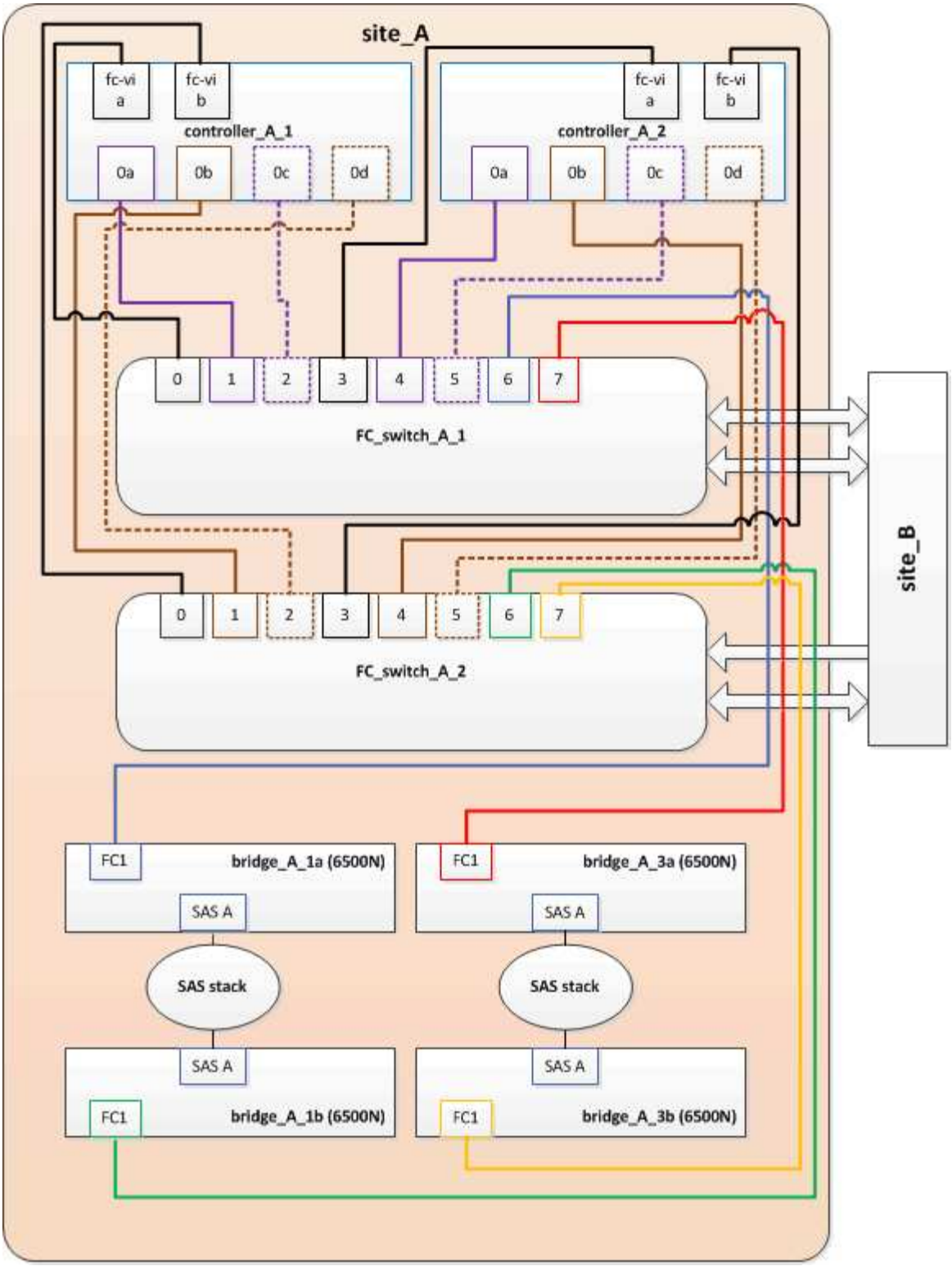
O zoneamento deve ser alterado quando você estiver substituindo as pontes FibreBridge 6500N por pontes FibreBridge 7500N e usando ambas as portas FC nas pontes FibreBridge 7500N. Cada zona não pode ter mais de quatro portas de iniciador. O zoneamento que você usa depende se você está executando o ONTAP antes da versão 9,1 ou 9,1 e posterior

Sobre esta tarefa

O zoneamento específico nesta tarefa é para versões do ONTAP anteriores à versão 9,1.

As alterações de zoneamento são necessárias para evitar problemas com o ONTAP, o que requer que não mais de quatro portas de iniciador FC possam ter um caminho para um disco. Após a desativação para consolidar as gavetas, o zoneamento existente resultaria em cada disco ser acessível por oito portas FC. Você deve alterar o zoneamento para reduzir as portas do iniciador em cada zona para quatro.

O diagrama a seguir mostra o zoneamento no site_A antes das alterações:



Passos

1. Atualize as zonas de armazenamento dos switches FC removendo metade das portas do iniciador de cada zona existente e criando novas zonas para as portas do FibreBridge 7500N FC2.

   As zonas para as novas portas FC2 conterão as portas do iniciador removidas das zonas existentes. Nos diagramas, estas zonas são apresentadas com linhas tracejadas.

   Para obter detalhes sobre os comandos de zoneamento, consulte as seções de switch FC do "Instalação e configuração do MetroCluster conectado à malha" ou "Instalação e configuração do Stretch

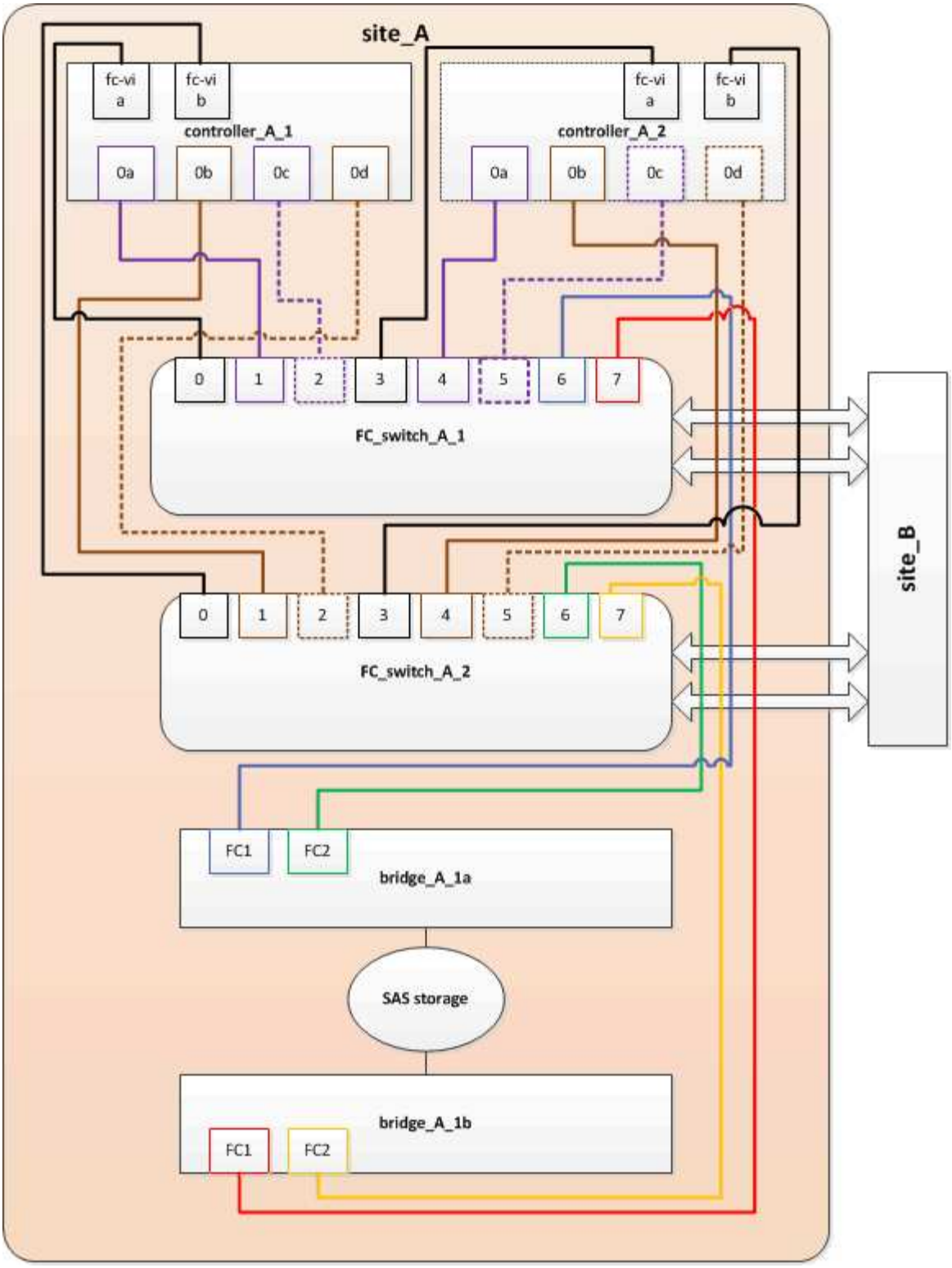
MetroCluster".

Os exemplos a seguir mostram as zonas de armazenamento e as portas em cada zona antes e depois da consolidação. As portas são identificadas por *domain, port* pairs.

- O domínio 5 consiste no switch FC_switch_A_1.
- O domínio 6 consiste no switch FC_switch_A_2.
- O domínio 7 consiste no switch FC_switch_B_1.
- O domínio 8 consiste no switch FC_switch_B_2.

Antes ou depois da consolidação	Zona	Domínios e portas	Cores nos diagramas (os diagramas mostram apenas o local A)
Zonas antes da consolidação. Há uma zona para cada porta FC nas quatro pontes FibreBridge 6500N.	STOR_A_1a-FC1	5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,6	Roxo, roxo e azul
STOR_A_1b-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,6	Castanho e castanho tracejado e verde	STOR_A_2a-FC1
5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,7	Roxo e vermelho	STOR_A_2b-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,7
Castanho e castanho tracejado e laranja	Zonas após a consolidação. Há uma zona para cada porta FC nas duas pontes FibreBridge 7500N.	STOR_A_1a-FC1	7,1; 7,4; 5,1; 5,4; 5,6
Roxo e azul	STOR_A_1b-FC1	7,2; 7,5; 5,2; 5,5; 5,7	Puré roxo e vermelho
STOR_A_1a-FC2	8,1; 8,4; 6,1; 6,4; 6,6	Castanho e verde	STOR_A_1b-FC2

O diagrama a seguir mostra zoneamento no site_A após a consolidação:



Atualizando zoneamento ao adicionar bridgeBridge 7600N ou 7500N bridges a uma configuração (ONTAP 9.1 e posterior)

O zoneamento deve ser alterado quando você estiver substituindo as pontes FibreBridge 6500N por pontes FibreBridge 7600N ou 7500N e usando ambas as portas FC nas pontes FibreBridge 7600N ou 7500N. Cada zona não pode ter mais de quatro portas de iniciador.

Sobre esta tarefa

- Esta tarefa aplica-se ao ONTAP 9.1 e posterior.
- As pontes FibreBridge 7600N são suportadas no ONTAP 9.6 e posterior.
- O zoneamento específico nesta tarefa é para o ONTAP 9.1 e posterior.
- As alterações de zoneamento são necessárias para evitar problemas com o ONTAP, o que requer que não mais de quatro portas de iniciador FC possam ter um caminho para um disco.

  Após a desativação para consolidar as gavetas, o zoneamento existente resultaria em cada disco ser acessível por oito portas FC. Você deve alterar o zoneamento para reduzir as portas do iniciador em cada zona para quatro.

Passo

1. Atualize as zonas de armazenamento dos switches FC removendo metade das portas do iniciador de cada zona existente e criando novas zonas para as portas FibreBridge 7600N ou 7500N FC2.

   As zonas para as novas portas FC2 conterão as portas do iniciador removidas das zonas existentes.

   Consulte a seção de switch FC de "Instalação e configuração do MetroCluster conectado à malha" para obter detalhes sobre os comandos de zoneamento.

Fazer o cabeamento da segunda porta FC de ponte ao adicionar pontes FibreBridge 7600N ou 7500N a uma configuração

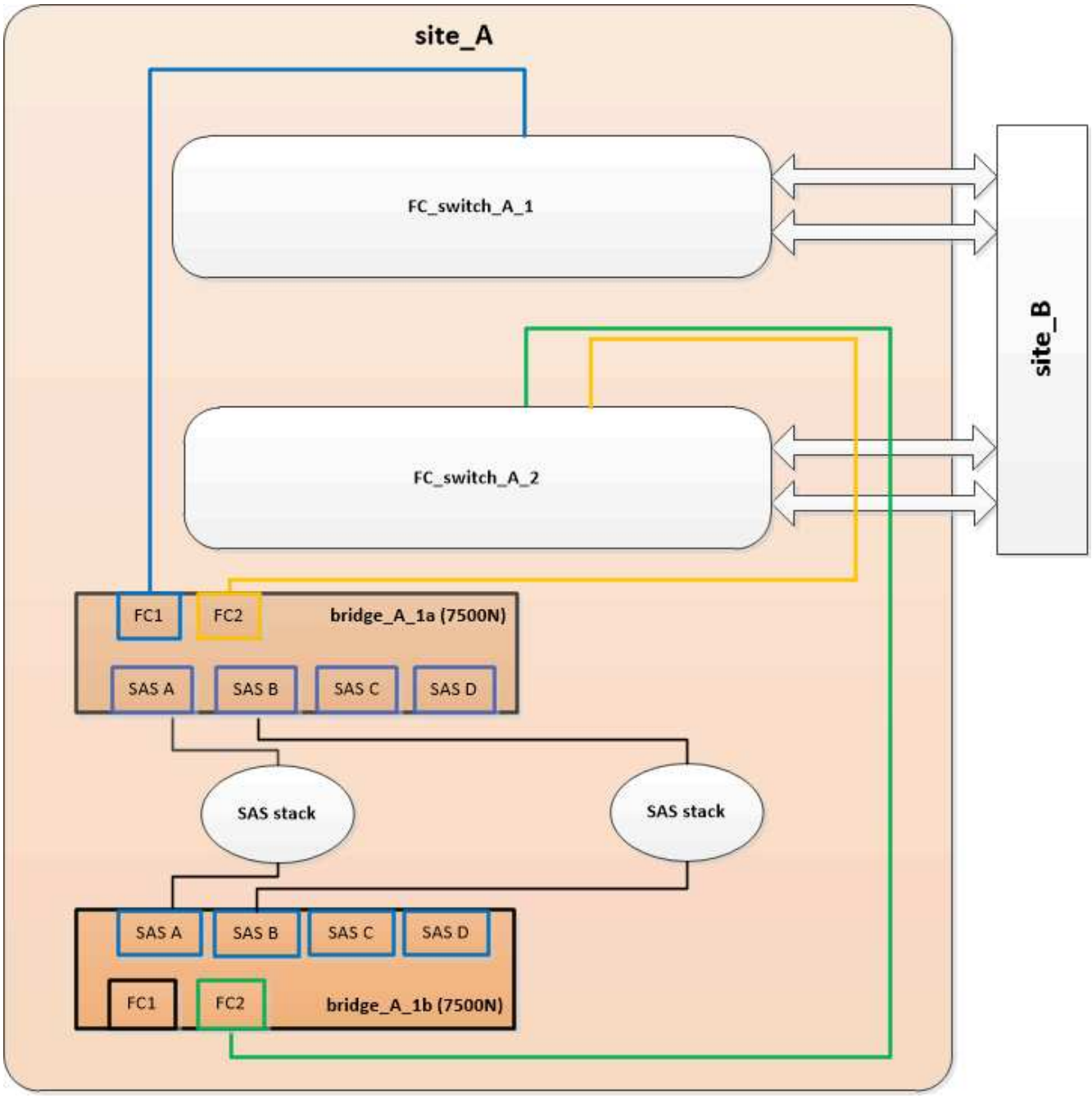
Para fornecer vários caminhos para as stacks de storage, você pode fazer o cabeamento da segunda porta FC em cada bridge do FibreBridge 7600N ou 7500N quando tiver adicionado a ponte FibreBridge 7600N ou 7500N à sua configuração.

Antes de começar

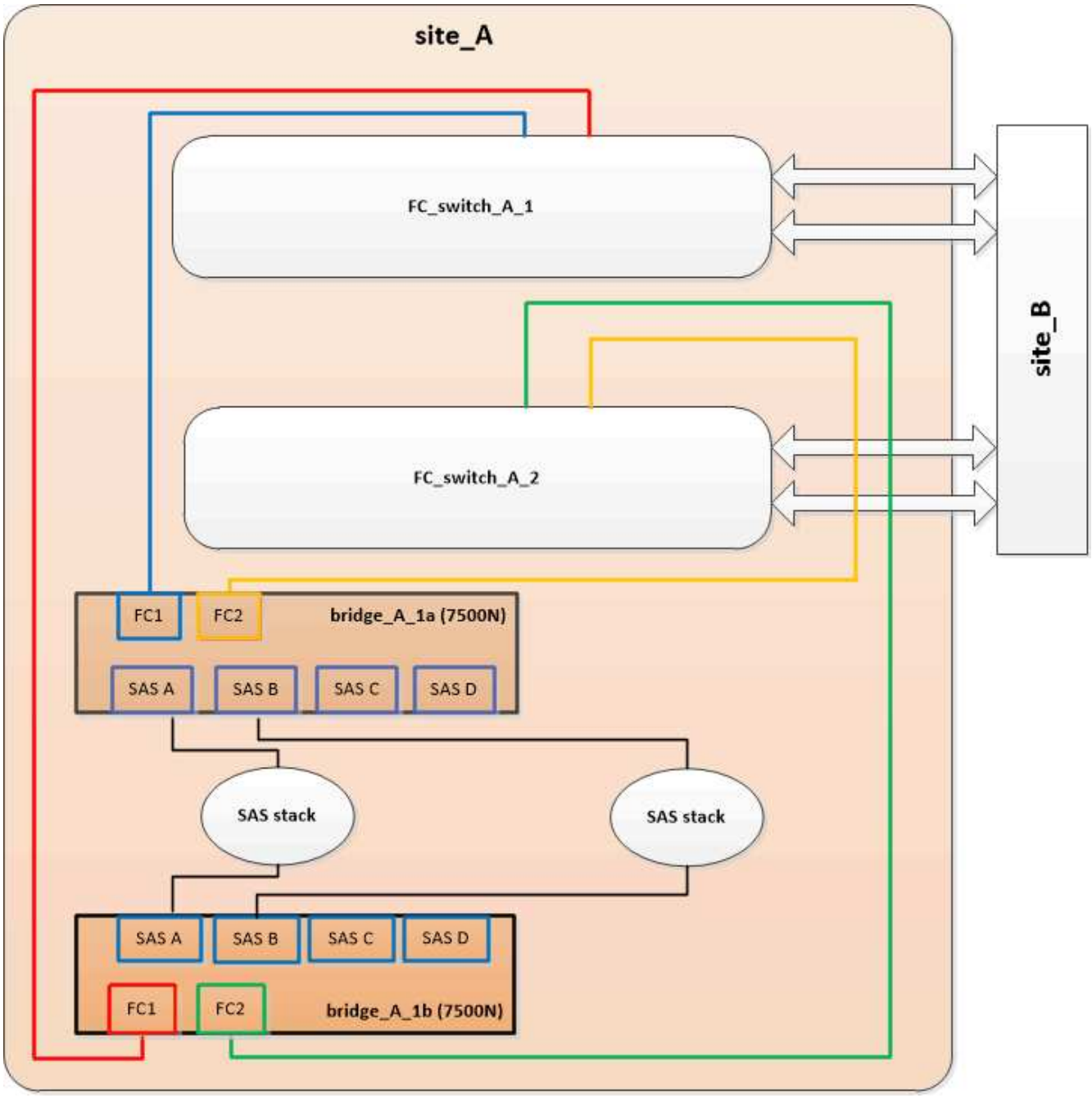
O zoneamento deve ter sido ajustado para fornecer zonas para as segundas portas FC.

Passos

1. Faça o cabo da porta FC2 da ponte superior para a porta correta no FC_switch_A_2.



2. Faça o cabo da porta FC1 da ponte inferior para a porta correta em FC_switch_A_1.



3. Confirme a conetividade com os discos conetados em ponte:

   `run local sysconfig -v`

   A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Desativação de portas SAS não usadas nas pontes FC para SAS

Depois de fazer alterações de cabeamento na ponte, você deve desativar todas as portas SAS não utilizadas em pontes FC para SAS para evitar alertas de monitor de integridade relacionados às portas não utilizadas.

Passos

1. Desative portas SAS não utilizadas na ponte FC para SAS superior:

   a. Faça login na ponte CLI.

   b. Desative quaisquer portas não utilizadas.

   > Se você tiver configurado uma ponte ATTO 7500N, todas as portas SAS (A a D) serão ativadas por padrão e você deverá desativar as portas SAS que não estão sendo usadas:
   >
   > `SASPortDisable` *`sas port`*

   Se as portas SAS A e B forem usadas, as portas SAS C e D devem ser desativadas. No exemplo a seguir, as portas SAS C e D não utilizadas são desativadas:

   ```
   Ready. *
   SASPortDisable C

   SAS Port C has been disabled.

   Ready. *
   SASPortDisable D

   SAS Port D has been disabled.

   Ready. *
   ```

   c. Salve a configuração da ponte
   `SaveConfiguration`

   O exemplo a seguir mostra que as portas SAS C e D foram desativadas. Observe que o asterisco não aparece mais, indicando que a configuração foi salva.

```
Ready. *
SaveConfiguration

Ready.
```

2. Repita a etapa anterior na ponte FC-para-SAS inferior.

Requisitos para usar outras interfaces para configurar e gerenciar bridges do FibreBridge

Você pode usar a combinação de uma porta serial, Telnet e FTP para gerenciar as bridges do FibreBridge em vez das interfaces de gerenciamento recomendadas. O sistema deve atender aos requisitos da interface aplicável antes de instalar as pontes.

Você pode usar uma porta serial ou Telnet para configurar a porta 1 de gerenciamento de bridge e Ethernet e gerenciar a ponte. Pode utilizar o FTP para atualizar o firmware da ponte.

O *ATTO FibreBridge Installation and Operation Manual* para sua ponte de modelo tem mais informações sobre interfaces de gerenciamento.

Você pode acessar este documento no SITE DA ATTO usando o link fornecido na página Descrição DO ATTO Fibrebridge.

Porta serial

Ao usar a porta serial para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet, o sistema deve atender aos seguintes requisitos:

- Um cabo serial (que se coneta da porta serial bridge a uma porta serial (com) no computador que você está usando para configuração)

  A porta serial bridge é RJ-45 e tem o mesmo pino-out que os controladores.

- Um programa de emulação de terminal como HyperTerminal, TeraTerm ou PuTTY para acessar o console

  O programa de terminal deve ser capaz de Registrar a saída de tela para um arquivo.

Telnet

Ao usar o Telnet para configurar e gerenciar uma bridge, o sistema deve atender aos seguintes requisitos:

- Um cabo serial (que se coneta da porta serial bridge a uma porta serial (com) no computador que você está usando para configuração)

  A porta serial bridge é RJ-45 e tem o mesmo pino-out que os controladores.

- (Recomendado) Um nome de usuário e senha não padrão (para acessar a ponte)
- Um programa de emulação de terminal como HyperTerminal, TeraTerm ou PuTTY para acessar o console

  O programa de terminal deve ser capaz de Registrar a saída de tela para um arquivo.

- Um endereço IP, máscara de sub-rede e informações de gateway para a porta 1 de gerenciamento Ethernet em cada bridge

FTP

Ao usar o FTP para atualizar o firmware da ponte, o sistema deve atender aos seguintes requisitos:

- Um cabo Ethernet padrão (que se coneta da porta 1 de gerenciamento Ethernet de ponte à sua rede)
- (Recomendado) Um nome de usuário e senha não padrão (para acessar a ponte)

Substituição a quente de um módulo de fonte de alimentação com falha

Quando há uma alteração no status de um módulo de fonte de alimentação para a ponte, você pode remover e instalar o módulo de fonte de alimentação.

Pode ver a alteração no estado de um módulo de fonte de alimentação através dos LEDs na ponte. Você também pode visualizar o status dos módulos de fonte de alimentação via ExpressNAV GUI e a ponte CLI, via porta serial ou via Telnet.

- Este procedimento é NDO (sem interrupções) e leva aproximadamente 15 minutos para ser concluído.
- Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

O *ATTO FibreBridge Installation and Operation Manual* para sua ponte de modelo tem mais informações sobre interfaces de gerenciamento.

Você pode acessar este e outros conteúdos no SITE DA ATTO usando o link fornecido na página Descrição DO ATTO Fibrebridge.

Gerenciamento na banda das pontes FC para SAS

Começando com o ONTAP 9.5 com o FibreBridge 7500N ou 7600N bridges, o gerenciamento em banda das pontes é suportado como uma alternativa ao gerenciamento IP das pontes. A partir do ONTAP 9.8, o gerenciamento fora da banda está obsoleto.

Sobre esta tarefa

A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Ao usar o gerenciamento na banda, as bridges podem ser gerenciadas e monitoradas a partir da CLI do ONTAP por meio da conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário, reduzindo a vulnerabilidade de segurança da ponte.

A disponibilidade do gerenciamento em banda das pontes depende da versão do ONTAP:

- A partir do ONTAP 9.8, as bridges são gerenciadas por meio de conexões na banda por padrão e o gerenciamento fora da banda das bridges via SNMP é obsoleto.
- ONTAP 9.5 a 9,7: O gerenciamento na banda ou o gerenciamento SNMP fora da banda é suportado.
- Antes do ONTAP 9.5, somente o gerenciamento SNMP fora da banda é suportado.

Os comandos Bridge CLI podem ser emitidos a partir do comando ONTAP interface `storage bridge run-cli -name` *`bridge-name`* `-command` *`bridge-command-name`* na interface ONTAP.

O uso do gerenciamento na banda com acesso IP desativado é recomendado para melhorar a segurança limitando a conetividade física da ponte.

Informações relacionadas

"Troca a quente de uma ponte com uma ponte de substituição do mesmo modelo"

"Troca quente de uma FibreBridge 7500N com uma ponte 7600N"

"Troca quente de uma ponte FibreBridge 6500N com uma ponte FibreBridge 7600N ou 7500N"

"Adição rápida de uma stack de compartimentos e bridges de disco SAS"

Gerenciamento de uma ponte FibreBridge a partir de ONTAP

A partir do ONTAP 9.5, você pode usar a CLI do ONTAP para passar os comandos do FibreBridge para a bridge e exibir os resultados desses comandos.

Sobre esta tarefa

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. Execute o comando FibreBridge aplicável dentro do `storage bridge run-cli` comando:

   `storage bridge run-cli -name` *`bridge-name`* `-command` *`"command-text"`*

   O seguinte comando executa o comando FibreBridge `SASPortDisable` a partir do prompt ONTAP para desativar a porta SAS b na ponte:

   ```
   cluster_A::> storage bridge run-cli -name "SASPortDisable b"

   SAS Port B has been disabled.
   Ready
   cluster_A::>
   ```

Fixar ou desprender a ponte FibreBridge

Para desativar facilmente protocolos Ethernet potencialmente inseguros em uma ponte, começando com o ONTAP 9.5, você pode proteger a ponte. Isto desativa as portas Ethernet da ponte. Você também pode reativar o acesso Ethernet.

- A proteção da ponte desativa os protocolos e serviços de porta telnet e de outras portas IP (FTP, ExpressNAV, ICMP ou Quicknav) na ponte.
- Este procedimento usa gerenciamento fora da banda usando o prompt ONTAP, que está disponível a partir do ONTAP 9.5.

  Você pode emitir os comandos da CLI de bridge se não estiver usando o gerenciamento fora da banda.

- O **`unsecurebridge`** comando pode ser usado para reativar as portas Ethernet.
- No ONTAP 9.7 e anteriores, executar o **`securebridge`** comando no FibreBridge ATTO pode não atualizar o status da ponte corretamente no cluster de parceiros. Se isso ocorrer, execute o **`securebridge`** comando do cluster de parceiros.

A partir de ONTAP 9.8, o **`storage bridge`** comando é substituído por **`system bridge`**. As etapas a seguir mostram o **`storage bridge`** comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o **`system bridge`** comando é preferido.

Passos

1. A partir do prompt ONTAP do cluster que contém a ponte, proteja ou desprenda a ponte.

   O seguinte comando protege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   securebridge
   ```

   O comando a seguir desprotege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   unsecurebridge
   ```

2. No prompt ONTAP do cluster que contém a ponte, salve a configuração da ponte:

   `storage bridge run-cli -bridge *bridge-name* -command saveconfiguration`

   O seguinte comando protege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. No prompt ONTAP do cluster que contém a ponte, reinicie o firmware da ponte:

   `storage bridge run-cli -bridge *bridge-name* -command firmwarerestart`

   O seguinte comando protege bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   firmwarerestart
   ```

Manutenção e substituição do comutador FC

Atualizando ou baixando o firmware em um switch Brocade FC

Para atualizar ou fazer downgrade do firmware em um switch Brocade FC, você deve usar os comandos específicos do Brocade para desativar o switch, executar e verificar a alteração de firmware e reinicializar e reativar o switch.

Sobre esta tarefa

Confirme se você verificou e executou as seguintes tarefas para sua configuração:

- Você tem os arquivos de firmware.
- O sistema está devidamente cabeado.
- Todos os caminhos para as gavetas de storage estão disponíveis.
- As pilhas do compartimento de disco são estáveis.
- A malha do switch FC está saudável.
- Não existem componentes com falha no sistema.
- O sistema está a funcionar normalmente.
- Você tem a senha de administrador e acesso a um servidor FTP ou SCP.
- O registo da consola está ativado.

  "Ativar o registo da consola"

A malha do switch é desativada durante uma atualização ou downgrade de firmware, e a configuração do MetroCluster depende da segunda malha para continuar a operação.

A partir do Fabric os 9,0.1, o SNMPv2 não é suportado nos switches Brocade. Se você atualizar para o Fabric os 9.0.1 ou posterior, use o SNMPv3 para monitoramento de integridade. Para obter mais informações, "Configurando o SNMPv3 em uma configuração MetroCluster"consulte .

Essa tarefa deve ser executada em cada uma das malhas de switch sucessivamente para que todos os switches estejam executando a mesma versão de firmware.

Esse procedimento não causa interrupções e leva aproximadamente uma hora para ser concluído.

Passos

1. Faça login em cada um dos switches da malha.

   Os exemplos nas etapas a seguir usam o switch `FC_switch_A_1`.

2. Desative cada um dos switches na estrutura:

   `switchCfgPersistentDisable`

   Se este comando não estiver disponível, execute o `switchDisable` comando.

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. Transfira a versão de firmware pretendida:

   `firmwareDownload`

   Quando solicitado o nome do arquivo, você deve especificar o subdiretório ou caminho relativo para o arquivo de firmware.

   Você pode executar o `firmwareDownload` comando ao mesmo tempo em ambos os switches, mas você

deve permitir que o firmware baixe e confirme corretamente antes de passar para a próxima etapa.

```
FC_switch_A_1:admin> firmwaredownload
Server Name or IP Address: 10.64.203.188
User Name: test
File Name: v7.3.1b
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password:
Server IP: 10.64.203.188, Protocol IPv4
Checking system settings for firmwaredownload...
System settings check passed.
```

4. Verifique se o firmware foi baixado e comprometido com ambas as partições:

   `firmwareShow`

   O exemplo a seguir mostra que a transferência do firmware está concluída à medida que ambas as imagens são atualizadas:

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. Reinicie os switches:

   `reboot`

   Algumas versões de firmware executam automaticamente uma operação de hahReboot depois que o download do firmware é concluído. A reinicialização nesta etapa é necessária mesmo que o haReboot tenha sido executado.

```
FC_switch_A_1:admin> reboot
```

6. Verifique se o novo firmware é para um nível de firmware intermediário ou para uma versão final especificada.

   Se o download for para o nível intermediário de firmware, execute as duas etapas anteriores até que a versão especificada seja instalada.

7. Ativar os interrutores:

   `switchCfgPersistentEnable`

Se este comando não estiver disponível, então o interrutor deve estar no `enabled` estado após `reboot` a execução do comando.

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. Verifique se os switches estão online e se todos os dispositivos estão conetados corretamente:

   `switchShow`

```
FC_switch_A_1:admin> switchShow
```

9. Verifique se as informações de uso do buffer para um grupo de portas ou todos os grupos de portas no switch são exibidas corretamente:

   `portbuffershow`

```
FC_switch_A_1:admin> portbuffershow
```

10. Verifique se a configuração atual de uma porta é exibida corretamente:

    `portcfgshow`

```
FC_switch_A_1:admin> portcfgshow
```

    Verifique as configurações da porta, como velocidade, modo, entroncamento, criptografia e compactação, na saída ISL (Inter-Switch Link). Verifique se as configurações da porta não foram afetadas pelo download do firmware.

11. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed
       `node run -node node-name sysconfig -a`
    b. Verifique se há alertas de integridade em ambos os clusters
       `system health alert show`
    c. Confirme a configuração do MetroCluster e se o modo operacional está normal
       `metrocluster show`
    d. Execute uma verificação MetroCluster
       `metrocluster check run`
    e. Exibir os resultados da verificação MetroCluster
       `metrocluster check show`
    f. Verifique se existem alertas de estado nos interrutores (se presentes)
       `storage switch show`
    g. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

12. Aguarde 15 minutos antes de repetir este procedimento para a segunda tela do interrutor.

Atualizando ou baixando o firmware em um switch Cisco FC

Para atualizar ou fazer o downgrade do firmware em um switch Cisco FC, você deve usar os comandos específicos do Cisco para desativar o switch, executar e verificar a atualização, reinicializar e reativar o switch.

Sobre esta tarefa

Confirme se você verificou e executou as seguintes tarefas para sua configuração:

- O sistema está devidamente cabeado.
- Todos os caminhos para as gavetas de storage estão disponíveis.
- As pilhas do compartimento de disco são estáveis.
- A malha do switch FC está saudável.
- Todos os componentes do sistema são saudáveis.
- O sistema está a funcionar normalmente.
- Você tem a senha de administrador e acesso a um servidor FTP ou SCP.
- O registo da consola está ativado.

"Ativar o registo da consola"

A malha do switch é desativada durante a atualização ou downgrade do firmware e a configuração do MetroCluster depende da segunda malha para continuar a operação.

Você deve repetir essa tarefa em cada uma das malhas de switch sucessivamente para garantir que todos os switches estejam executando a mesma versão de firmware.

Tem de ter os ficheiros de firmware.

Esse procedimento não causa interrupções e leva aproximadamente uma hora para ser concluído.

Passos

1. Faça login em cada um dos switches da malha.

   Nos exemplos, os switches são chamados FC_switch_A_1 e FC_switch_B_1.

2. Determine se há espaço suficiente no diretório bootflash em cada switch:

   ```
   dir bootflash
   ```

   Caso contrário, exclua os arquivos de firmware indesejados usando o `delete bootflash:file_name` comando.

3. Copie os arquivos kickstart e do sistema para os switches:

   copy *source_filetarget_file*

   No exemplo a seguir, o arquivo kickstart (`m9200-s2ek9-kickstart-mz.5.2.1.bin`) e o arquivo do sistema (`m9200-s2ek9-mz.5.2.1.bin`) estão localizados no servidor FTP 10.10.10.55 `/firmware/` no caminho.

   O exemplo a seguir mostra os comandos emitidos em FC_switch_A_1:

   ```
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-
   mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin
   bootflash:m9200-s2ek9-mz.5.2.1.bin
   ```

4. Desative todos os VSANs em ambos os switches nesta malha.

   Use o seguinte procedimento para desativar as VSANs:

   a. Abra o terminal de configuração:

      config t

   b. Introduza: **vsan database**

   c. Verifique o estado das VSANs:

      show vsan

      Todos os VSANs devem estar ativos.

   d. Suspender as VSANs:

      vsan *vsan-num* suspend

      Exemplo: `vsan 10 suspend`

   e. Verifique novamente o estado dos VSANs:

      show vsan Todos os VSANs devem ser suspensos.

   f. Saia do terminal de configuração:

      end

   g. Salve a configuração.

      copy running-config startup-config

      O exemplo a seguir exibe a saída para FC_switch_A_1:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# vsan 1 suspend
FC_switch_A_1(config-vsan-db)# vsan 30 suspend
FC_switch_A_1(config-vsan-db)# vsan 40 suspend
FC_switch_A_1(config-vsan-db)# vsan 70 suspend
FC_switch_A_1(config-vsan-db)# vsan 80 suspend
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
FC_switch_A_1# show vsan
```

```
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan
```

5. Instale o firmware desejado nos switches:

   install all system bootflash:*systemfile_name* kickstart bootflash:*kickstartfile_name*

   O exemplo a seguir mostra os comandos emitidos em FC_switch_A_1:

```
FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin
kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
Enter Yes to confirm the installation.
```

6. Verifique a versão do firmware em cada switch para se certificar de que a versão correta foi instalada:

show version

7. Ative todos os VSANs em ambos os switches desta malha.

   Use o seguinte procedimento para ativar as VSANs:

   a. Abra o terminal de configuração:

      config t

   b. Introduza: **vsan database**

   c. Verifique o estado das VSANs:

      show vsan

      As VSANs devem ser suspensas.

   d. Ativar as VSANs:

      no vsan *vsan-num* suspend

      Exemplo: `no vsan 10 suspend`

   e. Verifique novamente o estado dos VSANs:

      show vsan

      Todos os VSANs devem estar ativos.

   f. Saia do terminal de configuração:

      end

   g. Guardar a configuração:

      copy running-config startup-config

      O exemplo a seguir exibe a saída para FC_switch_A_1:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
```

```
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# no vsan 1 suspend
FC_switch_A_1(config-vsan-db)# no vsan 30 suspend
FC_switch_A_1(config-vsan-db)# no vsan 40 suspend
FC_switch_A_1(config-vsan-db)# no vsan 70 suspend
FC_switch_A_1(config-vsan-db)# no vsan 80 suspend
FC_switch_A_1(config-vsan-db)#
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
```

```
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
```

8. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      node run -node *node-name* sysconfig -a

   b. Verifique se há alertas de integridade em ambos os clusters:

      system health alert show

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      metrocluster show

   d. Execute uma verificação MetroCluster:

      metrocluster check run

   e. Apresentar os resultados da verificação MetroCluster:

      metrocluster check show

   f. Verifique se existem alertas de estado nos interrutores (se presentes):

      storage switch show

g. Execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

9. Repita este procedimento para a segunda tela do interrutor.

Atualização para novos switches Brocade FC

Se estiver atualizando para novos switches Brocade FC, substitua os switches na primeira malha, verifique se a configuração MetroCluster está totalmente operacional e substitua os switches na segunda malha.

- A configuração do MetroCluster deve estar em bom estado e em funcionamento normal.
- As malhas de switch MetroCluster consistem em quatro switches Brocade.

  As ilustrações nos passos seguintes mostram os interrutores atuais.

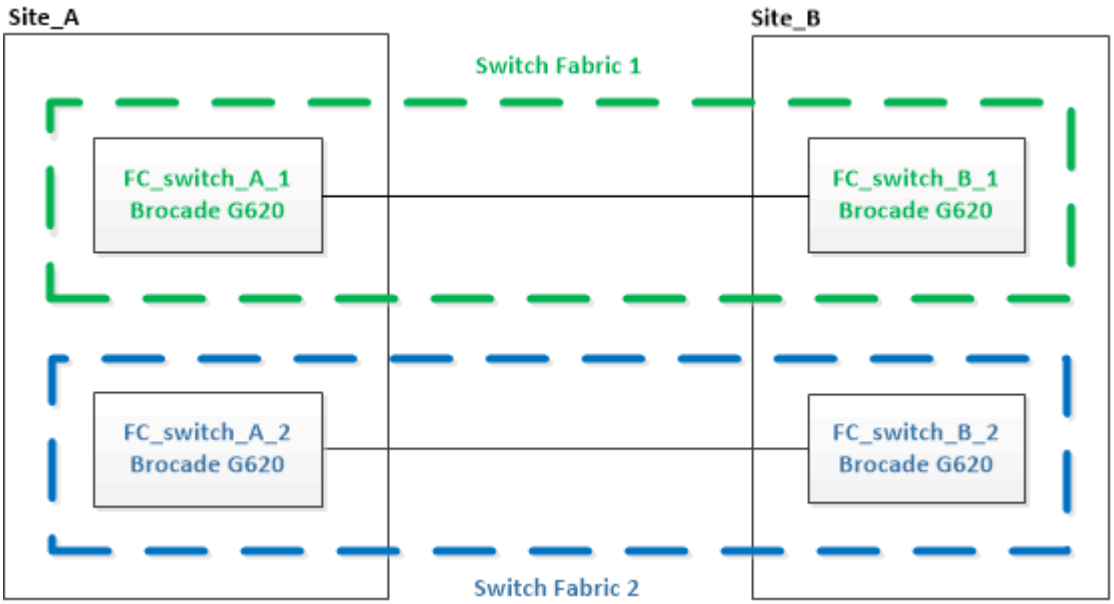
- Os switches devem estar executando o firmware suportado mais recente.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Esse procedimento não causa interrupções e leva aproximadamente duas horas para ser concluído.
- Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.
- "Ativar o registo da consola" antes de executar esta tarefa.

Os tecidos de troca são atualizados um de cada vez.

No final deste procedimento, todos os quatro interrutores serão atualizados para novos interrutores.

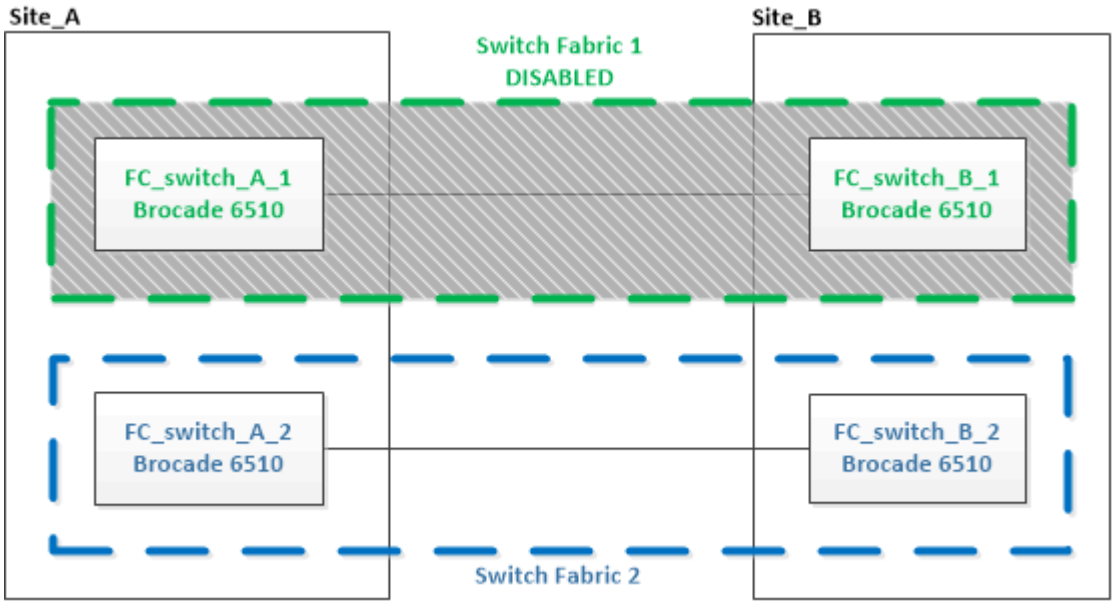


Passos

1. Desative o primeiro tecido do switch:

FC_switch_A_1:admin> switchCfgPersistentDisable

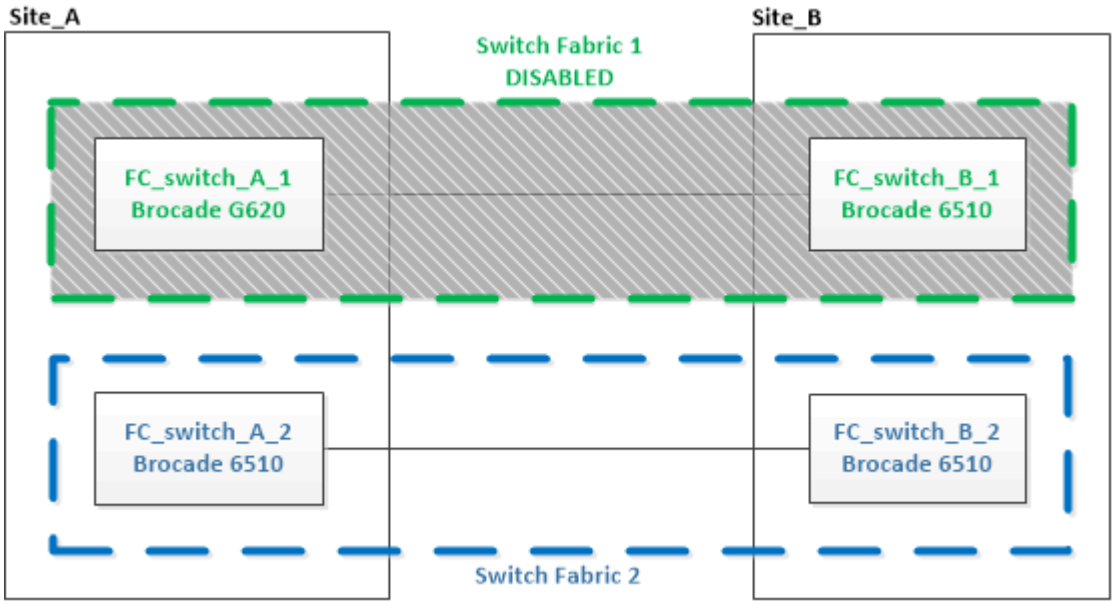
```
FC_switch_A_1:admin> switchCfgPersistentDisable
```



2. Substitua os interrutores antigos em um local do MetroCluster.

   a. Solte o cabo e retire o interrutor desativado.

   b. Instale o novo interrutor no rack.



   c. Desative os novos switches executando o seguinte comando em ambos os switches:

      `switchCfgPersistentDisable`

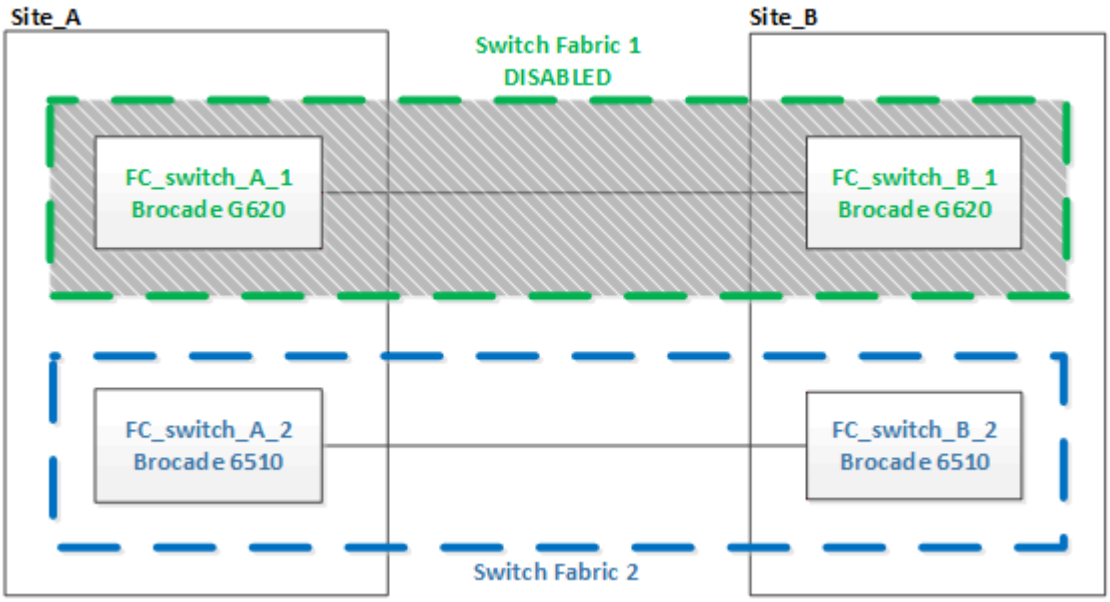
```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

d. Faça o cabo do novo switch usando as atribuições de portas recomendadas.

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

e. Repita essas subetapas no site do parceiro MetroCluster para substituir o segundo switch na primeira malha de switch.

Ambos os switches na malha 1 foram substituídos.



3. Ligue os novos interrutores e deixe-os arrancar.
4. Configure os switches Brocade FC usando um dos seguintes procedimentos:

"Configurar switches Brocade FC com arquivos RCF"

"Configure os switches Brocade FC manualmente"

5. Guardar a configuração do interrutor:

```
cfgSave
```

6. Aguarde 10 minutos para que a configuração se estabilize.
7. Confirme a conetividade com os discos inserindo o seguinte comando em qualquer um dos nós MetroCluster:

```
run local sysconfig -v
```

A saída mostra os discos conectados às portas do iniciador na controladora e identifica as gavetas conetadas às pontes FC para SAS:

```
node_A_1> run local sysconfig -v
```

```
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
```

```
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

8. Voltando ao prompt do switch, verifique a versão do firmware do switch:

   `firmwareShow`

   Os switches devem estar executando o firmware suportado mais recente.

   "Ferramenta de Matriz de interoperabilidade do NetApp"

9. Simular uma operação de comutação:

   a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado
   `set -privilege advanced`

      Você precisa responder com "'y'" quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   b. Efectuar a operação de comutação com o `-simulate` parâmetro:

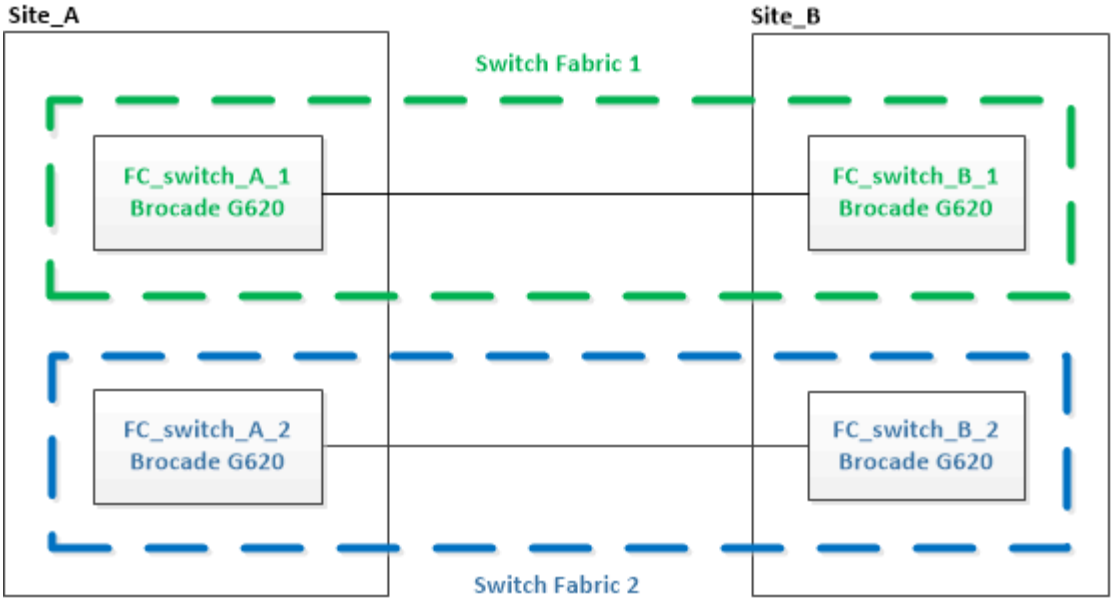
      `metrocluster switchover -simulate`

   c. Voltar ao nível de privilégio de administrador:

      `set -privilege admin`

10. Repita os passos anteriores no segundo tecido do interrutor.

Depois de repetir as etapas, todos os quatro switches foram atualizados e a configuração do MetroCluster está em operação normal.



Substituição de um switch Brocade FC

Você deve usar este procedimento específico do Brocade para substituir um switch com falha.

Sobre esta tarefa

Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

"Ativar o registo da consola" antes de executar esta tarefa.

Nos exemplos a seguir, FC_switch_A_1 é o interrutor de integridade e FC_switch_B_1 é o interrutor prejudicado. O uso da porta do switch nos exemplos é mostrado na tabela a seguir:

Ligações de portas	Portas
Conexões FC-VI	0, 3
Conexões HBA	1, 2, 4, 5
Conexões de ponte FC para SAS	6, 7
Conexões ISL	10, 11

Os exemplos mostram duas pontes FC-para-SAS. Se tiver mais, tem de desativar e, posteriormente, ativar as portas adicionais.

Esse procedimento não causa interrupções e leva aproximadamente duas horas para ser concluído.

O uso da porta do switch deve seguir as atribuições recomendadas.

- "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passos

1. Feche o interrutor que está sendo substituído desativando as portas ISL no interrutor de integridade na tela e as portas FC-VI e HBA no interrutor desativado (se o interrutor desativado ainda estiver funcionando):

   a. Desative as portas ISL no switch saudável para cada porta:

      `portcfgpersistentdisable` *`port-number`*

      ```
      FC_switch_A_1:admin> portcfgpersistentdisable 10
      FC_switch_A_1:admin> portcfgpersistentdisable 11
      ```

   b. Se o comutador desativado ainda estiver operacional, desative as portas FC-VI e HBA nesse comutador para cada porta:

      `portcfgpersistentdisable` *`port-number`*

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5
```

2. Se o interrutor desativado ainda estiver operacional, colete a saída do `switchshow` comando.

```
FC_switch_B_1:admin> switchshow
    switchName: FC_switch_B_1
    switchType: 71.2
    switchState:Online
    switchMode: Native
    switchRole: Subordinate
    switchDomain:       2
    switchId:   fffc01
    switchWwn:  10:00:00:05:33:86:89:cb
    zoning:             OFF
    switchBeacon:       OFF
```

3. Inicialize e pré-configure o novo switch antes de instalá-lo fisicamente:

   a. Ligue o novo interrutor e deixe-o arrancar.

   b. Verifique a versão do firmware no switch para confirmar que ela corresponde à versão dos outros switches FC:

      `firmwareShow`

c. Configure o novo switch seguindo as etapas em "Configure os switches Brocade FC manualmente".

> Neste ponto, o novo switch não é cabeado para a configuração do MetroCluster.

d. Desative as portas FC-VI, HBA e storage no novo switch e as portas conetadas às pontes FC-SAS.

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5

FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. Substitua fisicamente o interrutor:
   a. Desligue o interrutor FC desativado.
   b. Desligue o interrutor FC de substituição.
   c. Solte o cabo e retire o interrutor desativado, observando cuidadosamente quais cabos estão conetados a quais portas.
   d. Instale o interrutor de substituição no rack.
   e. Cabo o interrutor de substituição exatamente como o interrutor antigo foi cabeado.
   f. Ligue o novo switch FC.
5. Se pretender ativar a encriptação ISL, conclua as tarefas aplicáveis no "Instalação e configuração do MetroCluster conectado à malha".

   Se estiver a ativar a encriptação ISL, terá de concluir as seguintes tarefas:

   - Desative a malha virtual
   - Defina a carga útil
   - Defina a política de autenticação
   - Ativar a encriptação ISL nos comutadores Brocade
6. Conclua a configuração do novo interrutor:
   a. Ativar as ISLs:

      `portcfgpersistentenable` *`port-number`*

      ```
      FC_switch_B_1:admin> portcfgpersistentenable 10
      FC_switch_B_1:admin> portcfgpersistentenable 11
      ```

   b. Verifique a configuração de zoneamento:

```
cfg show
```

c. No comutador de substituição (FC_switch_B_1 no exemplo), verifique se os ISLs estão online:

```
switchshow
```

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

d. Habilite as portas de storage que se conetam às pontes FC.

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

e. Habilite o storage, as portas HBA e FC-VI.

O exemplo a seguir mostra os comandos usados para habilitar as portas que conetam adaptadores HBA:

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

O exemplo a seguir mostra os comandos usados para habilitar as portas que conetam os adaptadores FC-VI:

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

7. Verifique se as portas estão online:

   `switchshow`

8. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      `node run -node node-name sysconfig -a`

   b. Verifique se há alertas de integridade em ambos os clusters:

      `system health alert show`

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

   d. Execute uma verificação MetroCluster:

      `metrocluster check run`

   e. Apresentar os resultados da verificação MetroCluster:

      `metrocluster check show`

   f. Verifique se existem alertas de estado nos interrutores (se presentes):

      `storage switch show`

   g. "Config Advisor"Executar .
   h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Renomeando um switch Brocade FC

Talvez seja necessário renomear um switch Brocade FC para garantir uma nomenclatura consistente em toda a configuração.

Sobre esta tarefa

"Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Desative persistentemente o interrutor ou interrutores em uma estrutura:

   `switchcfgpersistentdisable`

   O exemplo a seguir mostra a saída para o **`switchcfgpersistentdisable`** comando:

```
7840_FCIP_2:admin> switchcfgpersistentdisable
Switch's persistent state set to 'disabled'
2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840_FCIP_2, VE
Tunnel 24 is DEGRADED.
2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840_FCIP_2, VE
Tunnel 24 is OFFLINE.

7840_FCIP_2:admin>
```

2. Mudar o nome do interrutor ou interrutores:

   switchname *new-switch-name*

   Se você estiver renomeando ambos os switches na malha, use o mesmo comando em cada switch.

   O exemplo a seguir mostra a saída para o **switchname *new-switch-name*** comando:

```
7840_FCIP_2:admin> switchname FC_switch_1_B
Committing configuration...
Done.
Switch name has been changed.Please re-login into the switch for the
change to be applied.
2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B,
Switch name has been successfully changed to FC_switch_1_B.
7840_FCIP_2:admin>
```

3. Reinicie o interrutor ou interrutores:

   reboot

   Se você estiver renomeando ambos os switches na malha, reinicie ambos os switches. Quando a reinicialização estiver concluída, o switch será renomeado em todos os lugares.

   O exemplo a seguir mostra a saída para o **reboot** comando:

```
7840_FCIP_2:admin> reboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840,
System is about to reload.
Rebooting! Fri Mar  9 07:42:11 CET 2018

Broadcast message from root (ttyS0) Fri Mar  9 07:42:11 2018...

The system is going down for reboot NOW !!
INIT: Switching to runlevel: 6
INIT:
2018/03/09-07:50:48, [ESM-1013], 146104, FID 128, INFO, FC_switch_1_B,
DP0 Configuration replay has completed.
2018/03/09-07:50:48, [ESM-1011], 146105, FID 128, INFO, FC_switch_1_B,
DP0 is ONLINE.

*** CORE FILES WARNING (03/09/18 - 08:00:00 ) ***
10248 KBytes in 1 file(s)
use "supportsave" command to upload


*** FFDC FILES WARNING (03/09/18 - 08:00:00 ) ***
520 KBytes in 1 file(s)
```

4. Ativar persistentemente os interrutores: **`switchcfgpersistentenable`**

   O exemplo a seguir mostra a saída para o **`switchcfgpersistentenable`** comando:

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch's persistent state set to 'enabled'
FC_switch_1_B:admin>
FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128,
INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B,
VE Tunnel 24 is ONLINE.

FC_switch_1_B:admin>


FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address  Media Speed   State       Proto
==================================================
   0   0   060000   id    16G     Online      FC  F-Port
50:0a:09:81:06:a5:5a:08
   1   1   060100   id    16G     Online      FC  F-Port
50:0a:09:83:06:a5:5a:08
```

5. Verifique se a alteração do nome do switch está visível no prompt do cluster do ONTAP:

   `storage switch show`

   O exemplo a seguir mostra a saída para o **`storage switch show`** comando:

```
cluster_A::*> storage switch show
  (storage switch show)
                      Symbolic                                    Is
Monitor
Switch                Name     Vendor  Model Switch WWN       Monitored
Status
--------------------- -------- ------- ----- ---------------- ---------
-------
Brocade_172.20.7.90
                      RTP-FC01-510Q40
                               Brocade Brocade7840
                                            1000c4f57c904bc8 true
ok
Brocade_172.20.7.91
                      RTP-FC02-510Q40
                               Brocade Brocade7840
                                            100050eb1a9aa579 true
ok
Brocade_172.20.7.92
```

Desativação da criptografia em switches Brocade FC

Talvez seja necessário desativar a criptografia em switches Brocade FC.

Passos

1. Envie uma mensagem AutoSupport de ambos os locais indicando o início da manutenção.

```
cluster_A::> autosupport invoke -node * -type all -message MAINT=4h
```

```
cluster_B::> autosupport invoke -node * -type all -message MAINT=4h
```

2. Verifique a operação da configuração do MetroCluster a partir do cluster A..
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal
   `metrocluster show`

```
cluster_A::> metrocluster show
```

   b. Execute uma verificação MetroCluster
   `metrocluster check run`

```
cluster_A::> metrocluster check run
```

c. Exibir os resultados da verificação MetroCluster
metrocluster check show

```
cluster_A::> metrocluster check show
```

3. Verifique o estado de ambos os interrutores:

fabric show

```
switch_A_1:admin> fabric show
```

```
switch_B_1:admin> fabric show
```

4. Desativar ambos os interrutores:

switchdisable

```
switch_A_1:admin> switchdisable
```

```
switch_B_1:admin> switchdisable
```

5. Verifique os caminhos disponíveis para os nós em cada cluster:

sysconfig

```
cluster_A::> system node run -node node-name -command sysconfig -a
```

```
cluster_B::> system node run -node node-name -command sysconfig -a
```

Como a malha do switch agora está desativada, a configuração de storage do sistema deve ser de caminho único HA.

6. Verifique o status agregado de ambos os clusters.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

A saída do sistema deve mostrar que os agregados são espelhados e normais para ambos os clusters:

```
mirrored,normal
```

7. Repita os seguintes subpassos a partir do prompt de administração em ambas as centrais.

   a. Mostrar quais portas são criptografadas
   portenccompshow

   ```
   switch_A_1:admin> portenccompshow
   ```

   b. Desativar a encriptação nas portas encriptadas
   portcfgencrypt – disable *port-number*

   ```
   switch_A_1:admin> portcfgencrypt --disable 40
   switch_A_1:admin> portcfgencrypt --disable 41
   switch_A_1:admin> portcfgencrypt --disable 42
   switch_A_1:admin> portcfgencrypt --disable 43
   ```

   c. Defina o tipo de autenticação para todos:

   authUtil --set -a all

```
switch_A_1:admin> authUtil --set -a all
```

   a. Defina a política de autenticação no switch. Como Desativado
   authutil --policy -sw off

   ```
   switch_A_1:admin> authutil --policy -sw off
   ```

   b. Defina o grupo Diffie-Hellman de autenticação como
   authutil --set -g *

   ```
   switch_A_1:admin> authUtil --set -g *
   ```

   c. Excluir o banco de dados de chaves secretas
   secAuthSecret --remove -all

```
switch_A_1:admin> secAuthSecret --remove -all
```

d. Confirme se a encriptação está desativada nas portas
portenccompshow

```
switch_A_1:admin> portenccompshow
```

e. Ativar o interrutor
switchenable

```
switch_A_1:admin> switchenable
```

f. Confirme o estado dos ISLs
islshow

```
switch_A_1:admin> islshow
```

8. Verifique os caminhos disponíveis para os nós em cada cluster:

sysconfig

```
cluster_A::> system node run -node * -command sysconfig -a
```

```
cluster_B::> system node run -node * -command sysconfig -a
```

A saída do sistema deve indicar que a Configuração de armazenamento do sistema mudou de volta para Quad-Path HA.

9. Verifique o status agregado de ambos os clusters.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

O sistema deve mostrar que os agregados são espelhados e normais para ambos os clusters, como mostrado na seguinte saída do sistema:

```
mirrored,normal
```

10. Verifique a operação da configuração do MetroCluster a partir do cluster A..

    a. Execute uma verificação MetroCluster
    metrocluster check run

    ```
    cluster_A::> metrocluster check run
    ```

    b. Exibir os resultados da verificação MetroCluster
    metrocluster check show

    ```
    cluster_A::> metrocluster check show
    ```

11. Envie uma mensagem AutoSupport de ambos os locais indicando o fim da manutenção.

    ```
    cluster_A::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

    ```
    cluster_B::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

Alterar propriedades ISL, portas ISL ou a configuração IOD/OOD em um switch Brocade

Talvez seja necessário adicionar ISLs a um switch se você estiver adicionando ou atualizando hardware, como controladores ou switches adicionais ou mais rápidos.

Antes de começar

Certifique-se de que o sistema está configurado corretamente, de que todos os switches de malha estão operacionais e de que não existem erros.

"Ativar o registo da consola" antes de executar esta tarefa.

Se o equipamento no link ISL mudar e a nova configuração de link não suportar mais a configuração atual----entroncamento e entrega ordenada----- então a malha precisa ser reconfigurada para a política de roteamento correta: Seja in-order-deliver (IOD) ou out-of-order-delivery (OOD).

> Para fazer alterações no software ODE a partir do ONTAP, siga estas etapas: "Configuração da entrega em ordem ou entrega fora de ordem de quadros no software ONTAP"

Passos

1. Desative as portas FCVI e HBA de armazenamento:

   `portcfgpersistentdisable` *`port number`*

   Por padrão, as primeiras portas 8 (portas 0 a 7) são usadas para FCVI e HBA de armazenamento. As portas devem ser persistentemente desativadas para que as portas permaneçam desativadas em caso de

reinicialização do switch.

O exemplo a seguir mostra que as portas ISL 0—7 estão sendo desativadas em ambos os switches:

```
Switch_A_1:admin> portcfgpersistentdisable 0-7
Switch_B_1:admin> portcfgpersistentdisable 0-7
```

2. Altere as portas ISL conforme necessário.

Opção	Passo
Para alterar a velocidade de uma porta ISL…	Use o `portcfgspeed` *`port number port speed`* comando em ambos os switches da malha. No exemplo a seguir, você altera a velocidade da porta ISL de 40 Gbps para 16 Gbps: `brocade_switch_A_1:admin> portcfgspeed 40 16` Você pode verificar se a velocidade foi alterada usando o `switchshow` comando: `brocade_switch_A_1:admin> switchshow` Você deve ver a seguinte saída: `. . .` `40 40 062800 id 16G No_Sync FC Disabled` `. . .`
Para alterar a distância de uma porta ISL…	Use o `portcfglongdistance` *`port number port distance`* comando em ambos os switches na malha.
Para remover um ISL…	Desligue a ligação.
Para adicionar um ISL…	Insira SFPs nas portas que você está adicionando como portas ISL. Certifique-se de que essas portas estejam listadas no "Instale um MetroCluster conectado à malha" para o switch ao qual você as está adicionando.
Para realocar um ISL…	Mudar um ISL é o mesmo que remover e, em seguida, adicionar um ISL. Primeiro, remova o ISL desconetanto o link e insira SFPs nas portas que você está adicionando como portas ISL.

Quando você faz alterações nas portas ISL, você também pode precisar aplicar configurações adicionais recomendadas pelo fornecedor do WDM. Consulte a documentação do fornecedor do WDM para obter orientação.

3. Reconfigure para entrega fora de encomenda (OOD) ou entrega em encomenda (IOD).

> Se as políticas de roteamento permanecerem as mesmas, você não precisará reconfigurar e essa etapa pode ser ignorada. A configuração do ONTAP precisa ser compatível com a configuração da malha. Se a malha estiver configurada para ODE, o ONTAP também deve ser configurado para ODE. O mesmo se aplica para IOD.

Esta etapa deve ser executada nos seguintes cenários:

- Mais de um ISL formou um tronco antes da alteração, mas após a alteração, o entroncamento não é mais suportado. Nesse caso, você deve configurar a malha para O ODE.
- Há um ISL antes da alteração e vários ISLs após a alteração.
- Se vários ISLs formarem um tronco, configure a malha para IOD. Se vários ISLs **não** formarem um tronco, configure a estrutura para OOD.
- Desative persistentemente os switches usando o `switchcfgpersistentdisable` comando como mostrado no exemplo a seguir:

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

i. Configure o modo de entroncamento para cada ISL `portcfgtrunkport` *`port number`* como mostrado na tabela a seguir:

Cenário	Passos
Configurar o ISL para entroncamento (IOD)	Defina o `portcfgtrunkport` *`port number`* para 1: `FC_switch_A_1:admin> portcfgtrunkport 20 1` `FC_switch_A_1:admin> portcfgtrunkport 21 1` `FC_switch_B_1:admin> portcfgtrunkport 20 1` `FC_switch_B_1:admin> portcfgtrunkport 21 1`
Configurar o ISL para entroncamento (OOD)	Defina o `portcfgtrunkport` *`port number`* para 0: `FC_switch_A_1:admin> portcfgtrunkport 20 0` `FC_switch_A_1:admin> portcfgtrunkport 21 0` `FC_switch_B_1:admin> portcfgtrunkport 20 0` `FC_switch_B_1:admin> portcfgtrunkport 21 0`

ii. Configure a malha para IOD ou ODE, conforme necessário.

Cenário	Passos

Configurar a malha para IOD	Defina as três configurações do IOD, APT e DLS usando os `iodset` comandos , `aptpolicypolicy` e , `dlsreset` como mostrado no exemplo a seguir: `Switch_A_1:admin> iodset` `Switch_A_1:admin> aptpolicy 1` `Policy updated successfully.` `Switch_A_1:admin> dlsreset` `FC_switch_A_1:admin>portcfgtrunkport 40 1` `FC_switch_A_1:admin>portcfgtrunkport 41 1` `Switch_B_1:admin> iodset` `Switch_B_1:admin> aptpolicy 1` `Policy updated successfully.` `Switch_B_1:admin> dlsreset` `FC_switch_B_1:admin>portcfgtrunkport 20 1` `FC_switch_B_1:admin>portcfgtrunkport 21 1`
Configurar a malha para ODE	Defina as três configurações do IOD, APT e DLS usando os `iodreset` comandos , `aptpolicy`*`policy`* e , `dlsset` como mostrado no exemplo a seguir: `Switch_A_1:admin> iodreset` `Switch_A_1:admin> aptpolicy 3` `Policy updated successfully.` `Switch_A_1:admin> dlsset` `FC_switch_A_1:admin> portcfgtrunkport 40 0` `FC_switch_A_1:admin> portcfgtrunkport 41 0` `Switch_B_1:admin> iodreset` `Switch_B_1:admin> aptpolicy 3` `Policy updated successfully.` `Switch_B_1:admin> dlsset` `FC_switch_B_1:admin> portcfgtrunkport 40 0` `FC_switch_B_1:admin> portcfgtrunkport 41 0`

iii. Ative os interrutores persistentemente:

`switchcfgpersistentenable`

```
switch_A_1:admin>switchcfgpersistentenable
switch_B_1:admin>switchcfgpersistentenable
```

+
Se este comando não existir, use o `switchenable` comando como mostrado no exemplo a seguir:

```
brocade_switch_A_1:admin>
switchenable
```

i. Verifique as configurações DO ODE usando os `iodshow` comandos , `aptpolicy` e `dlsshow` , conforme mostrado no exemplo a seguir:

```
switch_A_1:admin> iodshow
IOD is not set

switch_A_1:admin> aptpolicy

       Current Policy: 3 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

Você deve executar esses comandos em ambos os switches.

ii. Verifique as configurações IOD usando os `iodshow` comandos , `aptpolicy` e , `dlsshow` conforme mostrado no exemplo a seguir:

```
switch_A_1:admin> iodshow
IOD is set

switch_A_1:admin> aptpolicy
       Current Policy: 1 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is not set
```

Você deve executar esses comandos em ambos os switches.

4. Verifique se os ISLs estão on-line e truncados (se o equipamento de vinculação suportar entroncamento) usando os `islshow` comandos e. `trunkshow`

Se o FEC estiver ativado, o valor de desajuste da última porta on-line do grupo de troncos pode mostrar uma diferença de até 36, embora os cabos tenham o mesmo comprimento.

Os ISLs estão truncados?	Você vê a seguinte saída do sistema…
Sim	Se os ISLs forem truncados, apenas um ISL único aparece na saída para o `islshow` comando. A porta 40 ou 41 pode aparecer dependendo de qual é o tronco principal. A saída de `trunkshow` um tronco com ID "'1" que lista os ISLs físicos nas portas 40 e 41. No exemplo a seguir, as portas 40 e 41 são configuradas para uso como ISL: `switch_A_1:admin> islshow 1:` `40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 32.000G TRUNK CR_RECOV FEC` `switch_A_1:admin> trunkshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER` `41-> 41 10:00:00:05:33:88:9c:68 2 deskew 15`

Não	Se os ISLs não estiverem truncados, ambos os ISLs aparecerão separadamente nas saídas para `islshow` e `trunkshow`. Ambos os comandos listam os ISLs com sua ID de "'1" e "'2". No exemplo a seguir, as portas "'40'" e "'41'" são configuradas para uso como um ISL: `switch_A_1:admin> islshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC` `2: 41-> 41 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC` `switch_A_1:admin> trunkshow` `1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER` `2: 41-> 41 10:00:00:05:33:88:9c:68 2 deskew 48 MASTER`

5. Execute o `spinfab` comando em ambos os switches para verificar se os ISLs estão em boas condições:

```
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. Ative as portas que foram desativadas na etapa 1:

   `portenable` *`port number`*

   O exemplo a seguir mostra que as portas ISL "'0"" através de "'7" estão sendo ativadas:

```
brocade_switch_A_1:admin> portenable 0-7
```

Substituição de um switch Cisco FC

Você deve usar as etapas específicas do Cisco para substituir um switch Cisco FC com falha.

Antes de começar

Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

"Ativar o registo da consola" antes de executar esta tarefa.

Sobre esta tarefa

Esse procedimento não causa interrupções e leva aproximadamente duas horas para ser concluído.

Nos exemplos deste procedimento, FC_switch_A_1 é o interrutor de integridade e FC_switch_B_1 é o interrutor prejudicado. O uso da porta do switch nos exemplos é mostrado na tabela a seguir:

Função	Portas

Conexões FC-VI	1, 4
Conexões HBA	2, 3, 5, 6
Conexões de ponte FC para SAS	7, 8
Conexões ISL	36, 40

Os exemplos mostram duas pontes FC-para-SAS. Se tiver mais, tem de desativar e, posteriormente, ativar as portas adicionais.

O uso da porta do switch deve seguir as atribuições recomendadas.

- "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Passos

1. Desative as portas ISL no interrutor saudável para fechar o interrutor desativado.

   Estes passos são executados no interrutor de integridade.

   a. Entrar no modo de configuração
   `conf t`

   b. Desative as portas ISL no interrutor de integridade com os `interface` comandos e. `shut`

   ```
   FC_switch_A_1# conf t
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config)# shut
   FC_switch_A_1(config)# interface fc1/40
   FC_switch_A_1(config)# shut
   ```

   c. Saia do modo de configuração e copie a configuração para a configuração de inicialização.

   ```
   FC_switch_A_1(config)# end
   FC_switch_A_1# copy running-config startup-config
   FC_switch_A_1#
   ```

2. Feche as portas FC-VI e HBA no interrutor prejudicado (se ainda estiver em execução).

   Estes passos são realizados no interrutor desativado.

   a. Entre no modo de configuração:

   `conf t`

   b. Se o interrutor desativado ainda estiver operacional, desative as portas FC-VI e HBA no interrutor desativado com a interface e os comandos de desligamento.

```
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
```

c. Saia do modo de configuração e copie a configuração para a configuração de inicialização.

```
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. Se o interrutor desativado ainda estiver operacional, determine a WWN do interrutor:

   `show wwn switch`

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:e3:86:50
FC_switch_B_1#
```

4. Inicialize e pré-configure o comutador de substituição antes de o instalar fisicamente.

   Neste ponto, o switch de substituição não é cabeado para a configuração do MetroCluster. As portas ISL no switch parceiro são desativadas (no modo de corte) e offline.

   a. Ligue o interrutor de substituição e deixe-o arrancar.

   b. Verifique a versão do firmware no comutador de substituição para confirmar que corresponde à versão dos outros comutadores FC:

      `show version`

   c. Configure o switch de substituição conforme descrito no *Guia de Instalação e Configuração do MetroCluster*, ignorando a seção ""Configurando zoneamento em um switch Cisco FC"".

      "Instalação e configuração do MetroCluster conectado à malha"

   Você configurará o zoneamento mais tarde neste procedimento.

   a. Desative as portas FC-VI, HBA e armazenamento no comutador de substituição.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/7-8
FC_switch_B_1(config)# shut
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

5. Substitua fisicamente o interrutor desativado:
   a. Desligue o interrutor desativado.
   b. Desligue o interrutor de substituição.
   c. Solte o cabo e retire o interrutor desativado, observando cuidadosamente quais cabos estão conetados a quais portas.
   d. Instale o interrutor de substituição no rack.
   e. Cabo o interrutor de substituição exatamente como o interrutor desativado foi cabeado.
   f. Ligue o interrutor de substituição.
6. Ative as portas ISL no interrutor de substituição.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#
```

7. Verifique se as portas ISL no interrutor de substituição estão ativadas:

```
show interface brief
```

8. Ajuste o zoneamento no interrutor de substituição para corresponder à configuração do MetroCluster:
   a. Distribua as informações de zoneamento do tecido saudável.

      Neste exemplo, FC_switch_B_1 foi substituído e as informações de zoneamento são recuperadas de FC_switch_A_1:

```
FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end
```

b. No interrutor de substituição, verifique se as informações de zoneamento foram recuperadas adequadamente do interrutor de integridade:

`show zone`

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. Encontre as WWNs dos switches.

Neste exemplo, as duas WWNs de switch são as seguintes:

- FC_switch_A_1: 20:00:54:7f:EE:B8:24:C0
- FC_switch_B_1: 20:00:54:7f:EE:C6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

d. Remova os membros da zona que não pertencem ao switch WWNs dos dois switches.

   Neste exemplo, "nenhuma interface de membro" na saída mostra que os seguintes membros não estão associados ao switch WWN de qualquer um dos switches na malha e devem ser removidos:

   - Nome da zona FC-VI_Zone_1_10 vsan 10
     - a interface fc1/1 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/2 oscila 20:00:54:7f:ee:e3:86:50
   - Nome de zona STOR_Zone_1_20_25A vsan 20
     - a interface fc1/5 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/8 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/9 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/10 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/11 oscila 20:00:54:7f:ee:e3:86:50
   - Nome de zona STOR_Zone_1_20_25B vsan 20
     - a interface fc1/8 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/9 oscila 20:00:54:7f:ee:e3:86:50
     - a interface fc1/10 oscila 20:00:54:7f:ee:e3:86:50
     - Interface FC1/11 Swwn 20:00:54:7f:EE:e3:86:50 o exemplo a seguir mostra a remoção dessas interfaces:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

e. Adicione as portas do comutador de substituição às zonas.

   Todo o cabeamento do comutador de substituição deve ser igual ao do comutador desativado:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

f. Verifique se o zoneamento está configurado corretamente:

   `show zone`

   A saída de exemplo a seguir mostra as três zonas:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

g. Ative a conetividade ao storage e aos controladores.

   O exemplo a seguir mostra o uso da porta:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      `node run -node node-name sysconfig -a`

   b. Verifique se há alertas de integridade em ambos os clusters:

      `system health alert show`

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

   d. Execute uma verificação MetroCluster:

      `metrocluster check run`

   e. Apresentar os resultados da verificação MetroCluster:

      `metrocluster check show`

   f. Verifique se existem alertas de estado nos interrutores (se presentes):

      `storage switch show`

   g. Execute o Config Advisor.

      "NetApp Downloads: Config Advisor"

   h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Alteração da velocidade das portas ISL em um switch Cisco FC

Talvez seja necessário alterar a velocidade das portas ISL em um switch para melhorar a qualidade do ISL. ISLs viajando distâncias maiores podem precisar de sua velocidade

reduzida para melhorar a qualidade.

Sobre esta tarefa

- Conclua todas as etapas em ambos os switches para garantir a conetividade ISL.
- "Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Desative as portas ISL das ISLs que você deseja alterar a velocidade de em ambos os switches na malha:

   `FC_switch_A_1# config t`

   Introduza os comandos de configuração, um por linha. Termine com CTRL-Z depois de ter introduzido todos os comandos de configuração.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# shut
      FC_switch_A_1(config)# end
   ```

2. Altere a velocidade das portas ISL em ambos os interrutores na estrutura:

   `FC_switch_A_1# config t`

   Introduza os comandos de configuração, um por linha. Termine com CTRL-Z depois de ter introduzido todos os comandos de configuração.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# switchport speed 16000
   ```

   As velocidades para portas são de 16 Gbps, 16.000 Gbps, 8 Gbps, 8.000 Gbps, 4 Gbps, 4.000 Gbps.

   Certifique-se de que essas portas ISL para seu switch estejam listadas no *Fabric-Attached MetroCluster Installation and Configuration Guide*.

3. Ative todas as portas ISL (se não estiver ativado) em ambos os switches na estrutura:

   `FC_switch_A_1# config t`

   Introduza os comandos de configuração, um por linha. Termine com CTRL-Z depois de ter introduzido todos os comandos de configuração.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

4. Verifique se as ISLs estão estabelecidas entre ambos os switches:

show topology isl

```
------------------------------------------------------------------------
--------
    ___________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

5. Repita o procedimento para a segunda tela do interrutor.

Adicionando ISLs a um switch Cisco

Talvez seja necessário adicionar ISLs a um switch se você estiver adicionando ou atualizando hardware, como controladores adicionais ou mais rápidos ou switches mais rápidos.

Sobre esta tarefa

- Conclua todas as etapas em ambos os switches para garantir a conetividade ISL.
- "Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Desative as portas ISL das ISLs a serem adicionadas em ambos os switches na malha:

   FC_switch_A_1#config t

   Introduza os comandos de configuração, um por linha. Termine com CTRL-Z depois de todos os comandos de configuração terem sido introduzidos.

   ```
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end
   ```

2. Insira SFPs nas portas que você está adicionando como portas ISL, e faça o cabo deles de acordo com o *Installation and Configuration Guide*.

Verifique se essas portas estão listadas no *Installation and Configuration Guide* para o switch ao qual você as está adicionando.

3. Configure as portas ISL de acordo com o *Installation and Configuration Guide*.
4. Ative todas as portas ISL (se não estiver ativado) em ambos os switches na estrutura:

   FC_switch_A_1# config t

   Introduza os comandos de configuração, um por linha. Terminar com CTRL-Z.

   ```
   FC_switch_A_1# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

5. Verifique se as ISLs estão estabelecidas entre ambos os switches:

   show topology isl

6. Repita o procedimento no segundo tecido:

```
------------------------------------------------------------------------
--------
    ___________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

Alterar o fornecedor ou o modelo dos switches FC

Talvez seja necessário alterar o fornecedor de switches FC de Cisco para Brocade ou vice-versa, alterar o modelo do switch ou alterar ambos.

Sobre esta tarefa

- Este procedimento aplica-se quando você estiver usando switches validados pela NetApp.

- "Ativar o registo da consola" antes de executar esta tarefa.
- Siga as etapas deste procedimento em uma malha de cada vez, para ambas as malhas na configuração.

Passos

1. Verifique a integridade da configuração.
   a. Verifique se o MetroCluster está configurado e no modo normal em cada cluster: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verifique se o espelhamento está ativado em cada nó: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Verifique se os componentes do MetroCluster estão em bom estado: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Verifique se não existem alertas de saúde: **`system health alert show`**

2. Configure os novos switches antes da instalação.

   Siga as etapas em "Configurar os switches FC".

3. Desligar as ligações dos interrutores antigos, retirando as ligações pela seguinte ordem:
   a. Desconete as interfaces MetroCluster FC e FCVI.
   b. Desconete as pontes ATTO FibreBridge.
   c. Desligue os ISLs da MetroCluster.
4. Desligue os interrutores antigos, retire os cabos e substitua fisicamente os interrutores antigos pelo novo interrutor.
5. Faça o cabo dos interrutores pela seguinte ordem:

   Tem de seguir os passos em "Fazer o cabeamento de uma configuração MetroCluster conectada à malha".

   a. Faça o cabo das ISLs para o local remoto.
   b. Faça o cabo das pontes ATTO FibreBridge.
   c. Faça o cabeamento das interfaces MetroCluster FC e FCVI.
6. Ligue os interrutores.
7. Verifique se a configuração do MetroCluster está saudável repetindo [Passo 1].
8. Repita os passos 1 a 7 para a segunda estrutura na configuração.

Substituição de uma gaveta sem interrupções em uma configuração MetroCluster conectada à malha

Talvez seja necessário saber como substituir uma gaveta sem interrupções em uma

configuração MetroCluster conectada à malha.

Este procedimento é apenas para uso em uma configuração MetroCluster conetada à malha.

Desativando o acesso ao compartimento

Você deve desativar o acesso ao compartimento antes de substituir os módulos do compartimento.

Verifique a integridade geral da configuração. Se o sistema não parecer saudável, aborde o problema primeiro antes de prosseguir.

Passos

1. Em ambos os clusters, todos os plexos off-line com discos na pilha de gaveta afetada:

   `aggr offline plex_name`

   O exemplo mostra os comandos para offlining plexes para um controlador que executa OTNAP agrupado.

   ```
   cluster_A_1::> storage aggregate plex offline -aggr aggrA_1_0 -plex
   plex0
   cluster_A_1::> storage aggregate plex offline -aggr dataA_1_data -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr aggrA_2_0 -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr dataA_2_data -plex
   plex0
   ```

2. Verifique se os plexes estão offline:

   `aggr status -raggr_name`

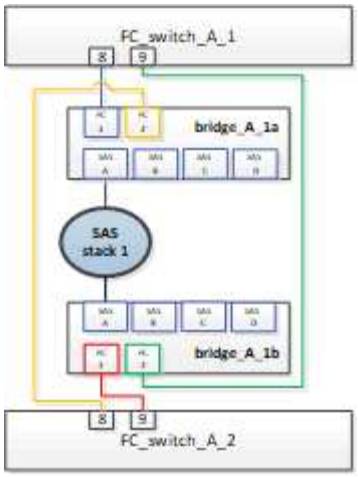
   O exemplo mostra os comandos para verificar se os agregados estão offline para uma controladora executando o cMode.

   ```
   Cluster_A_1::> storage aggregate show -aggr aggrA_1_0
   Cluster_A_1::> storage aggregate show -aggr dataA_1_data
   Cluster_A_2::> storage aggregate show -aggr aggrA_2_0
   Cluster_A_2::> storage aggregate show -aggr dataA_2_data
   ```

3. Desative as portas SAS ou as portas do switch dependendo se as pontes que conetam o compartimento de destino estão conetando uma única pilha SAS ou duas ou mais pilhas SAS:

   - Se as bridges estiverem conetando uma única pilha SAS, desative as portas do switch às quais as bridges estão conetadas usando o comando apropriado para o switch.

     O exemplo a seguir mostra um par de bridges que conetam uma única pilha SAS, que contém o compartimento de destino:



As portas de switch 8 e 9 em cada switch conetam as pontes à rede.

O exemplo a seguir mostra as portas 8 e 9 sendo desativadas em um switch Brocade.

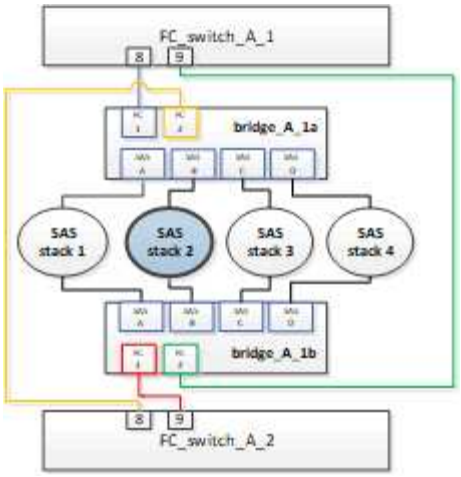
```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9

FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

O exemplo a seguir mostra as portas 8 e 9 sendo desativadas em um switch Cisco.

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

- Se as bridges estiverem conetando duas ou mais pilhas SAS, desative as portas SAS conetando as bridges ao compartimento de destino
`SASportDisable` *`port number`*

O exemplo a seguir mostra um par de bridges que conetam quatro stacks SAS. A pilha SAS 2 contém o compartimento de destino:



A porta SAS B coneta as pontes ao compartimento de destino. Ao desativar apenas a porta B SAS em ambas as gavetas, as outras stacks SAS podem continuar fornecendo dados durante o procedimento de substituição.

Nesse caso, desative a porta SAS conetando a ponte ao compartimento de destino:

`SASportDisable` *`port number`*

O exemplo a seguir mostra que a porta SAS B está sendo desativada da ponte e também verifica se ela está desativada. Você deve repetir o comando em ambas as pontes.

```
Ready. *
SASPortDisable B

SAS Port B has been disabled.
```

4. Se você desativou anteriormente as portas do switch, verifique se elas estão desativadas:

   `switchShow`

   O exemplo mostra que as portas do switch estão desativadas em um switch Brocade.

   ```
   FC_switch_A_1:admin> switchShow
   FC_switch_A_2:admin> switchShow
   ```

   O exemplo mostra que as portas do switch estão desativadas em um switch Cisco.

   ```
   FC_switch_A_1# show interface fc1/6
   FC_switch_A_2# show interface fc1/6
   ```

5. Aguarde que o ONTAP perceba que o disco está faltando.
6. Desligue a gaveta que você deseja substituir.

Substituição da prateleira

Você precisa remover fisicamente todos os cabos e a gaveta antes de inserir e fazer o cabeamento dos novos módulos de gaveta e gaveta.

Passos

1. Remova todos os discos e desconete todos os cabos da prateleira que está sendo substituída.
2. Retire os módulos das prateleiras.
3. Insira a nova prateleira.
4. Insira os novos discos na nova gaveta.
5. Insira os módulos das prateleiras.
6. Cable a gaveta (SAS ou alimentação).
7. Ligue a prateleira.

Reativando o acesso e verificando a operação

Após a substituição do compartimento, você precisa reativar o acesso e verificar se o novo compartimento está funcionando corretamente.

Passos

1. Verifique se a gaveta é alimentada corretamente e se os links nos módulos IOM estão presentes.
2. Ative as portas do switch ou a porta SAS de acordo com os seguintes cenários:

Opção	Passo

Se você desativou anteriormente as portas do switch	a. Ativar as portas do switch: `portEnable port number` O exemplo mostra a porta do switch sendo ativada em um switch Brocade. ``` Switch_A_1:admin> portEnable 6 Switch_A_2:admin> portEnable 6 ``` O exemplo mostra a porta do switch sendo ativada em um switch Cisco. ``` Switch_A_1# conf t Switch_A_1(config)# int fc1/6 Switch_A_1(config)# no shut Switch_A_1(config)# end Switch_A_2# conf t Switch_A_2(config)# int fc1/6 Switch_A_2(config)# no shut Switch_A_2(config)# end ```
Se você desativou anteriormente uma porta SAS	a. Habilite a porta SAS conetando a pilha ao local do compartimento: `SASportEnable port number` O exemplo mostra que a porta SAS A está sendo ativada a partir da ponte e também verifica se ela está ativada. ``` Ready. * SASPortEnable A SAS Port A has been enabled. ```

3. Se você desativou anteriormente as portas do switch, verifique se elas estão ativadas e on-line e se todos os dispositivos estão conetados corretamente:

   `switchShow`

   O exemplo mostra o `switchShow` comando para verificar se um switch Brocade está on-line.

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

O exemplo mostra o `switchShow` comando para verificar se um switch Cisco está on-line.

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

Após vários minutos, o ONTAP deteta que novos discos foram inseridos e exibe uma mensagem para cada novo disco.

4. Verifique se os discos foram detetados pelo ONTAP:

   `sysconfig -a`

5. Online os plexes que estavam offline anteriormente:

   `aggr online`*`plex_name`*

   O exemplo mostra os comandos para colocar plexes em um controlador executando cMode de volta on-line.

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

   Os plexos começam a ressincronizar.

Você pode monitorar o progresso da ressincronização usando o `aggr status -r`*`aggr_name`* comando.

Adicionar storage a uma configuração MetroCluster FC

Adição automática de um compartimento de disco SAS em uma configuração de MetroCluster FC com conexão direta usando cabos óticos SAS

Você pode usar cabos óticos SAS para adicionar um compartimento de disco SAS a uma stack existente de gavetas de disco SAS em uma configuração de MetroCluster FC com conexão direta ou como uma nova stack de um HBA SAS ou uma porta SAS integrada na controladora.

- Esse procedimento não causa interrupções e leva aproximadamente duas horas para ser concluído.
- Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.
- Se estiver adicionando uma gaveta de IOM12 TB a uma stack de IOM6 gavetas, "Adição automática de IOM12 gavetas a uma stack de IOM6 gavetas"consulte .

Essa tarefa se aplica a uma configuração de FC MetroCluster na qual o storage é conetado diretamente às controladoras de storage com cabos SAS. Isso não se aplica a configurações de FC MetroCluster que usam pontes FC para SAS ou malhas de switches FC.

Passos

1. Siga as instruções para adicionar um compartimento de disco SAS a quente no *Installation Guide* para o modelo de compartimento de disco para executar as seguintes tarefas para adicionar um compartimento de disco a quente:
   a. Instale um compartimento de disco para adicionar um hot-add.
   b. Ligue as fontes de alimentação e defina a ID do compartimento para adicionar um hot-add.
   c. Coloque o cabo na gaveta de disco hot-Added.
   d. Verifique a conetividade SAS.

Adicionar storage SAS a uma configuração MetroCluster FC conetada em ponte

Adição rápida de uma stack de gavetas de disco SAS a um par existente de bridgeBridge 7600N ou 7500N

É possível adicionar uma stack de gavetas de disco SAS a um par existente de bridgeBridge 7600N ou 7500N que tenha portas disponíveis.

Antes de começar

- Você deve ter baixado o firmware mais recente do compartimento de disco e disco.
- Todos os compartimentos de disco na configuração MetroCluster (compartimentos existentes) devem estar executando a mesma versão de firmware. Se um ou mais discos ou gavetas não estiverem executando a versão de firmware mais recente, atualize o firmware antes de anexar os novos discos ou gavetas.

  "Downloads do NetApp: Firmware da unidade de disco"

  "Downloads do NetApp: Firmware da gaveta de disco"

- As pontes FibreBridge 7600N ou 7500N devem estar conetadas e ter portas SAS disponíveis.

Sobre esta tarefa

Este procedimento é escrito com a suposição de que você está usando as interfaces de gerenciamento de bridge recomendadas: A GUI ATTO ExpressNAV e o utilitário ATTO Quicknav.

Você pode usar a GUI ATTO ExpressNAV para configurar e gerenciar uma bridge e atualizar o firmware da bridge. Você pode usar o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet bridge.

Você pode usar outras interfaces de gerenciamento, se necessário. Essas opções incluem o uso de uma porta serial ou Telnet para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet e usar o FTP para atualizar o firmware da ponte. Se você escolher qualquer uma dessas interfaces de gerenciamento, deverá atender aos requisitos aplicáveis no "Outras interfaces de gerenciamento de ponte".

> Se você inserir um cabo SAS na porta errada, ao remover o cabo de uma porta SAS, deverá aguardar pelo menos 120 segundos antes de conetar o cabo a uma porta SAS diferente. Se não o fizer, o sistema não reconhecerá que o cabo foi movido para outra porta.

Passos

1. Aterre-se corretamente.
2. No console de qualquer controlador, verifique se o sistema tem atribuição automática de disco ativada:

   ```
   storage disk option show
   ```

A coluna atribuição automática indica se a atribuição automática de disco está ativada.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

3. Em cada bridge no par, ative a porta SAS que se conetará à nova pilha:

   `SASPortEnable` *`port-letter`*

   A mesma porta SAS (B, C ou D) deve ser usada em ambas as pontes.

4. Salve a configuração e reinicie cada bridge:

   `SaveConfiguration Restart`

5. Prenda as prateleiras de discos às pontes:

   a. Encadeie em série as gavetas de disco em cada pilha.

      O *Installation and Service Guide* do modelo de compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.

   b. Para cada stack de gavetas de disco, cable IOM A da primeira gaveta para a porta SAS a na FibreBridge A e, em seguida, cable IOM B da última gaveta para a porta SAS a na FibreBridge B.

      "Instalação e configuração do MetroCluster conectado à malha"

      "Instalação e configuração do Stretch MetroCluster"

      Cada ponte tem um caminho para sua pilha de gavetas de disco; a ponte A se coneta ao lado A da pilha através da primeira gaveta e a ponte B se coneta ao lado B da pilha através da última gaveta.

      ⓘ A porta SAS da ponte B está desativada.

6. Verifique se cada bridge pode detetar todas as unidades de disco e compartimentos de disco aos quais a ponte está conetada.

Se você estiver usando o…	Então…

ATTO ExpressNAV GUI	a. Em um navegador da Web compatível, insira o endereço IP de uma ponte na caixa do navegador. Você é trazido para a página inicial DO ATTO FibreBridge, que tem um link. b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte. A página de status ATTO FibreBridge aparece com um menu à esquerda. c. Clique em **Avançado** no menu. d. Ver os dispositivos ligados: `sastargets` e. Clique em **Enviar**.
Conexão de porta serial	Ver os dispositivos ligados: `sastargets`

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos.

Se o texto "Esponse truncado" aparecer no início da saída, você pode usar o Telnet para conetar-se à ponte e, em seguida, exibir toda a saída usando o `sastargets` comando.

A saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

7. Verifique se a saída do comando mostra que a ponte está conetada a todos os discos e compartimentos de disco apropriados na pilha.

Se a saída for…	Então…

Correto	Repita o passo anterior para cada ponte restante.
Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo a etapa para fazer o cabeamento das gavetas de disco às pontes. b. Repita o passo anterior para cada ponte restante.

8. Atualize o firmware da unidade de disco para a versão mais atual a partir da consola do sistema:

   `disk_fw_update`

   Você deve executar este comando em ambos os controladores.

   "Downloads do NetApp: Firmware da unidade de disco"

9. Atualize o firmware do compartimento de disco para a versão mais atual usando as instruções para o firmware baixado.

   Você pode executar os comandos no procedimento a partir do console do sistema de qualquer controlador.

   "Downloads do NetApp: Firmware da gaveta de disco"

10. Se o sistema não tiver a atribuição automática de disco ativada, atribua a propriedade da unidade de disco.

    "Gerenciamento de disco e agregado"

    Se você estiver dividindo a propriedade de uma única pilha de compartimentos de disco entre vários controladores, desative a atribuição automática de disco (`storage disk option modify -autoassign off *`de ambos os nós no cluster) antes de atribuir a propriedade de disco; caso contrário, quando você atribuir qualquer unidade de disco, as unidades de disco restantes podem ser atribuídas automaticamente ao mesmo controlador e pool.

    Não é possível adicionar unidades de disco a agregados ou volumes até que o firmware da unidade de disco e do compartimento de disco tenham sido atualizados e as etapas de verificação nesta tarefa tenham sido concluídas.

11. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed:

       `node run -node node-name sysconfig -a`

    b. Verifique se há alertas de integridade em ambos os clusters:

       `system health alert show`

    c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

       `metrocluster show`

d. Execute uma verificação MetroCluster:

```
metrocluster check run
```

e. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

f. Verifique se há alertas de integridade nas pontes depois de adicionar as novas pilhas:

```
storage bridge show
```

g. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

12. Se aplicável, repita este procedimento para o local do parceiro.

Adição rápida de uma stack de shelves de disco SAS e bridges a um sistema MetroCluster

Você pode adicionar sem interrupções (adicionar sem interrupções) uma stack inteira, incluindo pontes, ao sistema MetroCluster. Deve haver portas disponíveis nos switches FC e você deve atualizar o zoneamento do switch para refletir as alterações.

Sobre esta tarefa

- Esse procedimento pode ser usado para adicionar uma pilha usando bridges FibreBridge 7600N ou 7500N.
- Este procedimento é escrito com a suposição de que você está usando as interfaces de gerenciamento de bridge recomendadas: A GUI ATTO ExpressNAV e o utilitário ATTO Quicknav.
  - Você usa a GUI ATTO ExpressNAV para configurar e gerenciar uma bridge e atualizar o firmware da bridge. Você usa o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet bridge.
  - Você pode usar outras interfaces de gerenciamento, se necessário. Essas opções incluem o uso de uma porta serial ou Telnet para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet e usar o FTP para atualizar o firmware da ponte. Se você escolher qualquer uma dessas interfaces de gerenciamento, seu sistema precisará atender aos requisitos aplicáveis na "Outras interfaces de gerenciamento de ponte"

Preparando-se para adicionar uma stack de compartimentos e bridges de disco SAS

A preparação para adicionar uma stack de gavetas de disco SAS e um par de bridges envolve o download de documentos, bem como o firmware da unidade de disco e do compartimento de disco.

Antes de começar

- Seu sistema deve ser uma configuração com suporte e ter uma versão com suporte do ONTAP.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Todas as unidades de disco e compartimentos de disco no sistema devem estar executando a versão de firmware mais recente.

Talvez você queira atualizar o firmware do disco e do compartimento em toda a configuração do MetroCluster antes de adicionar gavetas.

"Atualize, reverta ou downgrade"

- Cada switch FC precisa ter uma porta FC disponível para que uma ponte seja conetada a ele.

  Talvez seja necessário atualizar o switch FC dependendo da compatibilidade do switch FC.

- O computador que você está usando para configurar as bridges deve estar executando um navegador da Web compatível com ATTO para usar a GUI ATTO ExpressNAV: Internet Explorer 8 ou 9, ou Mozilla Firefox 3.

  As Notas de versão do produto *ATTO* têm uma lista atualizada de navegadores da Web compatíveis. Pode aceder a este documento utilizando as informações apresentadas nos passos.

Passos

1. Faça o download ou veja os seguintes documentos no site de suporte da NetApp:
   - "Ferramenta de Matriz de interoperabilidade do NetApp"
   - O *Guia de Instalação e Serviço* para o modelo de compartimento de disco.
2. Faça o download do conteúdo do site DA ATTO e do site da NetApp:
   a. Vá para a página Descrição DO ATTO FibreBridge.
   b. Usando o link na página Descrição DO ATTO FibreBridge, acesse o site DA ATTO e faça o download do seguinte:
      - *ATTO FibreBridge Manual de Instalação e operação* para o seu modelo de ponte.
      - Utilitário ATTO Quicknav (para o computador que você está usando para configuração).
   c. Vá para a página Download de firmware do ATTO FibreBridge clicando em **continuar** no final da página Descrição DO ATTO FibreBridge e faça o seguinte:
      - Transfira o ficheiro de firmware da ponte conforme indicado na página de transferência.

        Nesta etapa, você só está completando a parte de download das instruções fornecidas nos links. Você atualiza o firmware em cada bridge mais tarde, quando instruído a fazê-lo na "Adicionando a pilha de prateleiras" seção.

      - Faça uma cópia da página de download do firmware DO ATTO FibreBridge e as notas de versão para referência posterior.
3. Faça download do firmware mais recente do disco e do compartimento de disco e faça uma cópia da parte de instalação das instruções para referência posterior.

   Todos os compartimentos de disco na configuração MetroCluster (as novas gavetas e as gavetas existentes) devem estar executando a mesma versão de firmware.

   Nesta etapa, você só está completando a parte de download das instruções fornecidas nos links e fazendo uma cópia das instruções de instalação. Você atualiza o firmware em cada disco e compartimento de disco mais tarde, quando instruído a fazê-lo na "Adicionando a pilha de prateleiras" seção.

   a. Faça download do firmware do disco e faça uma cópia das instruções de firmware do disco para referência posterior.

"Downloads do NetApp: Firmware da unidade de disco"

b. Faça download do firmware do compartimento de disco e faça uma cópia das instruções de firmware do compartimento de disco para referência posteriormente.

"Downloads do NetApp: Firmware da gaveta de disco"

4. Reúna o hardware e as informações necessárias para usar as interfaces de gerenciamento de bridge recomendadas - a GUI ATTO ExpressNAV e o utilitário ATTO Quicknav:
   a. Adquira um cabo Ethernet padrão para conetar a partir da porta 1 de gerenciamento Ethernet de ponte à sua rede.
   b. Determine um nome de usuário e uma senha não padrão para acessar as bridges.

      Recomenda-se que altere o nome de utilizador e a palavra-passe predefinidos.

   c. Obtenha um endereço IP, uma máscara de sub-rede e informações de gateway para a porta 1 de gerenciamento Ethernet em cada bridge.
   d. Desative os clientes VPN no computador que você está usando para configuração.

      Os clientes VPN ativos fazem com que o Quicknav procure por bridges falhem.

5. Adquira quatro parafusos para cada ponte para montar corretamente os suportes da ponte na parte frontal do rack.

   As aberturas nos suportes da ponte "L" estão em conformidade com o padrão de rack ETA-310-X para racks de 19 polegadas (482,6 mm).

6. Se necessário, atualize o zoneamento do switch FC para acomodar as novas pontes que estão sendo adicionadas à configuração.

   Se você estiver usando os arquivos de Configuração de Referência fornecidos pelo NetApp, as zonas foram criadas para todas as portas, portanto, você não precisa fazer atualizações de zoneamento. Deve haver uma zona de storage para cada porta do switch que se conete às portas FC da ponte.

Adição rápida de uma stack de compartimentos e bridges de disco SAS

É possível adicionar uma stack de shelves e bridges de disco SAS para aumentar a capacidade das pontes.

O sistema precisa atender a todos os requisitos para adicionar uma stack de shelves e bridges de disco SAS.

"Preparando-se para adicionar uma stack de compartimentos e bridges de disco SAS"

- Adicionar sem interrupções uma stack de shelves e bridges de disco SAS é um procedimento sem interrupções se todos os requisitos de interoperabilidade forem atendidos.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

  "Usando a ferramenta Matriz de interoperabilidade para encontrar informações do MetroCluster"

- O multipath HA é a única configuração suportada para sistemas MetroCluster que usam bridges.

  Ambos os módulos de controladora devem ter acesso por meio das pontes aos compartimentos de disco em cada stack.

- Você deve adicionar um número igual de compartimentos de disco em cada local.
- Se você estiver usando o gerenciamento na banda da ponte em vez do gerenciamento IP, as etapas para configurar a porta Ethernet e as configurações IP podem ser ignoradas, como observado nas etapas relevantes.

A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Se você inserir um cabo SAS na porta errada, ao remover o cabo de uma porta SAS, deverá aguardar pelo menos 120 segundos antes de conetar o cabo a uma porta SAS diferente. Se não o fizer, o sistema não reconhecerá que o cabo foi movido para outra porta.

Passos

1. Aterre-se corretamente.
2. No console de qualquer módulo do controlador, verifique se o sistema tem atribuição automática de disco ativada:

   `storage disk option show`

   A coluna atribuição automática indica se a atribuição automática de disco está ativada.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

3. Desative as portas do switch para a nova pilha.
4. Se estiver configurando para gerenciamento na banda, conete um cabo da porta serial FibreBridge RS-232 à porta serial (com) em um computador pessoal.

   A conexão serial será usada para configuração inicial e, em seguida, o gerenciamento na banda via ONTAP e as portas FC podem ser usados para monitorar e gerenciar a ponte.

5. Se estiver configurando para gerenciamento IP, configure a porta 1 de gerenciamento Ethernet para cada bridge seguindo o procedimento na seção 2,0 do *ATTO FibreBridge Installation and Operation Manual* para o modelo de bridge.

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

   Ao executar o Quicknav para configurar uma porta de gerenciamento Ethernet, apenas a porta de gerenciamento Ethernet conetada pelo cabo Ethernet é configurada. Por exemplo, se você também quiser configurar a porta 2 de gerenciamento Ethernet, será necessário conetar o cabo Ethernet à porta 2 e executar o Quicknav.

6. Configure a ponte.

Se você recuperou as informações de configuração da ponte antiga, use as informações para configurar a nova ponte.

Certifique-se de anotar o nome de utilizador e a palavra-passe que designou.

O *ATTO FibreBridge Installation and Operation Manual* para o seu modelo de bridge tem as informações mais atuais sobre os comandos disponíveis e como usá-los.

> Não configure a sincronização de tempo no ATTO FibreBridge 7600N ou 7500N. A sincronização de tempo para O ATTO FibreBridge 7600N ou 7500N é definida para a hora do cluster depois que a ponte é descoberta pelo ONTAP. Também é sincronizado periodicamente uma vez por dia. O fuso horário utilizado é GMT e não é variável.

a. Se estiver configurando para gerenciamento de IP, configure as configurações IP da ponte.

   Para definir o endereço IP sem o utilitário Quicknav, você precisa ter uma conexão serial com o FibreBridge.

   Se estiver usando a CLI, você deve executar os seguintes comandos:

   ```
   set ipaddress mp1 ip-address

   set ipsubnetmask mp1 subnet-mask

   set ipgateway mp1 x.x.x.x

   set ipdhcp mp1 disabled

   set ethernetspeed mp1 1000
   ```

b. Configure o nome da ponte.

   As pontes devem ter um nome exclusivo dentro da configuração do MetroCluster.

   Exemplos de nomes de bridge para um grupo de pilha em cada local:

   - bridge_A_1a
   - bridge_A_1b
   - bridge_B_1a
   - Bridge_B_1b se estiver usando a CLI, você deve executar o seguinte comando:

     ```
     set bridgename bridgename
     ```

c. Se estiver executando o ONTAP 9.4 ou anterior, ative o SNMP na ponte
   `set SNMP enabled`

   Em sistemas que executam o ONTAP 9.5 ou posterior, o gerenciamento na banda pode ser usado para acessar a ponte através das portas FC em vez da porta Ethernet. A partir do ONTAP 9.8, somente o gerenciamento na banda é suportado e o gerenciamento SNMP é obsoleto.

7. Configurar as portas FC de ponte.

a. Configure a taxa/velocidade de dados das portas FC em ponte.

   A taxa de dados FC suportada depende da ponte do modelo.

   - A ponte FibreBridge 7600N suporta até 32, 16 ou 8 Gbps.
   - A ponte FibreBridge 7500N suporta até 16, 8 ou 4 Gbps.

   > A velocidade FCDataRate selecionada é limitada à velocidade máxima suportada pela ponte e pelo switch ao qual a porta de ponte se coneta. As distâncias de cabeamento não devem exceder as limitações dos SFPs e de outro hardware.

   Se estiver usando a CLI, você deve executar o seguinte comando:

   `set FCDataRate port-number port-speed`

b. Se você estiver configurando uma ponte FibreBridge 7500N, configure o modo de conexão que a porta usa para "ptp".

   > A configuração FCConnMode não é necessária ao configurar uma ponte FibreBridge 7600N.

   Se estiver usando a CLI, você deve executar o seguinte comando:

`set FCConnMode port-number ptp`

a. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, você deve configurar ou desativar a porta FC2.
   - Se estiver usando a segunda porta, repita as subetapas anteriores para a porta FC2.
   - Se você não estiver usando a segunda porta, então você deve desativar a porta `FCPortDisable port-number`

b. Se você estiver configurando uma ponte FibreBridge 7600N ou 7500N, desative as portas SAS não utilizadas
`SASPortDisable sas-port`

   > As portas SAS De A a D estão ativadas por predefinição. Você deve desativar as portas SAS que não estão sendo usadas. Se apenas a porta SAS A for usada, as portas SAS B, C e D devem ser desativadas.

8. Proteja o acesso à ponte e salve a configuração da ponte.

   a. No prompt do controlador, verifique o status das pontes:

      `storage bridge show`

      A saída mostra qual ponte não está protegida.

   b. Verifique o estado das portas da ponte não protegida
   `info`

      A saída mostra o status das portas Ethernet MP1 e MP2.

c. Se a porta Ethernet MP1 estiver ativada, execute o seguinte comando
`set EthernetPort mp1 disabled`

> Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2.

d. Salve a configuração da ponte.

Você deve executar os seguintes comandos:

```
SaveConfiguration

FirmwareRestart
```

Você é solicitado a reiniciar a ponte.

9. Atualize o firmware do FibreBridge em cada ponte.

Se a nova ponte for do mesmo tipo que a ponte parceira atualize para o mesmo firmware que a ponte parceira. Se a nova ponte for um tipo diferente da ponte do parceiro, atualize para o firmware mais recente suportado pela ponte e versão do ONTAP. Consulte a seção "Atualizar firmware em uma ponte FibreBridge" em *Manutenção MetroCluster*.

10. Conete as prateleiras de disco às pontes:

a. Encadeie em série as gavetas de disco em cada pilha.

O *Installation Guide* para o modelo do seu compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.

b. Para cada stack de gavetas de disco, cable IOM A da primeira gaveta para a porta SAS a na FibreBridge A e, em seguida, cable IOM B da última gaveta para a porta SAS a na FibreBridge B.

"Instalação e configuração do MetroCluster conectado à malha"

"Instalação e configuração do Stretch MetroCluster"

Cada ponte tem um caminho para sua pilha de gavetas de disco; a ponte A se coneta ao lado A da pilha através da primeira gaveta e a ponte B se coneta ao lado B da pilha através da última gaveta.

> A porta SAS da ponte B está desativada.

11. Verifique se cada bridge pode detetar todas as unidades de disco e prateleiras de disco às quais a ponte está conetada.

Se você estiver usando o…	Então…

ATTO ExpressNAV GUI	a. Em um navegador da Web compatível, insira o endereço IP de uma ponte na caixa do navegador. Você é trazido para a página inicial DO ATTO FibreBridge, que tem um link. b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte. A página de status ATTO FibreBridge aparece com um menu à esquerda. c. Clique em **Avançado** no menu. d. Ver os dispositivos ligados `sastargets` e. Clique em **Enviar**.
Conexão de porta serial	Ver os dispositivos ligados: `sastargets`

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conetada. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os dispositivos.

Se a resposta de texto truncada aparecer no início da saída, você pode usar o Telnet para se conetar à ponte e, em seguida, exibir toda a saída usando o `sastargets` comando.

A saída a seguir mostra que 10 discos estão conetados:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

12. Verifique se a saída do comando mostra que a ponte está conetada a todos os discos e compartimentos de disco apropriados na pilha.

Se a saída for…	Então…
Correto	Repita Passo 11 para cada ponte restante.

Não está correto	a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo Passo 10. b. Repita Passo 11.

13. Se você estiver configurando uma configuração de MetroCluster conetada à malha, faça o cabeamento de cada bridge para os switches FC locais, usando o cabeamento mostrado na tabela para sua configuração, modelo de switch e modelo de ponte FC para SAS:

Os switches Brocade e Cisco usam numeração de portas diferente, como mostrado nas tabelas a seguir.

- Nos switches Brocade, a primeira porta é numerada ""0"".
- Nos switches Cisco, a primeira porta é numerada ""1"".

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)												
GRUPO DE RD 1												
			Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Componente		Porta	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2
Pilha 1	bridge_x_1a	FC1	8		8		8		8		10	
FC2	-	8	-	8	-	8	-	8	-	10	bridge_x_1B	FC1
9	-	9	-	9	-	9	-	11	-	FC2	-	9
-	9	-	9	-	9	-	11	Pilha 2	bridge_x_2a	FC1	10	-
10	-	10	-	10	-	14	-	FC2	-	10	-	10
-	10	-	10	-	14	bridge_x_2B	FC1	11	-	11	-	11
-	11	-	17	-	FC2	-	11	-	11	-	11	-

11	-	17	Pilha 3	bridge_x_3a	FC1	12	-	12	-	12	-	12
-	18	-	FC2	-	12	-	12	-	12	-	12	-
18	bridge_x_3B	FC1	13	-	13	-	13	-	13	-	19	-
FC2	-	13	-	13	-	13	-	13	-	19	Empilha y	bridge_x_ya
FC1	14	-	14	-	14	-	14	-	20	-	FC2	-
14	-	14	-	14	-	14	-	20	ponte_x_yb	FC1	15	-
15	-	15	-	15	-	21	-	FC2		15		15

Configurações usando o FibreBridge 7500N ou 7600N usando ambas as portas FC (FC1 e FC2)										
GRUPO DE RD 2										
			Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G720	
Componente		Porta	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	interruptor 2
Pilha 1	bridge_x_51a	FC1	26	-	32	-	56	-	32	-
FC2	-	26	-	32	-	56	-	32	bridge_x_51b	FC1
27	-	33	-	57	-	33	-	FC2	-	27
-	33	-	57	-	33	Pilha 2	bridge_x_52a	FC1	30	-
34	-	58	-	34	-	FC2	-	30	-	34
-	58	-	34	bridge_x_52b	FC1	31	-	35	-	59
-	35	-	FC2	-	31	-	35	-	59	-

35	Pilha 3	bridge_x_53a	FC1	32	-	36	-	60	-	36
-	FC2	-	32	-	36	-	60	-	36	bridge_x_53b
FC1	33	-	37	-	61	-	37	-	FC2	-
33	-	37	-	61	-	37	Empilha y	bridge_x_5ya	FC1	34
-	38	-	62	-	38	-	FC2	-	34	-
38	-	62	-	38	bridge_x_5yb	FC1	35	-	39	-
63	-	39	-	FC2	-	35	-	39	-	63

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)											
GRUPO DE RD 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Componente	Porta	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2	Interruptor 1	Interruptor 2
Pilha 1	bridge_x_1a	8		8		8		8		10	
bridge_x_1b	-	8	-	8	-	8	-	8	-	10	Pilha 2
bridge_x_2a	9	-	9	-	9	-	9	-	11	-	bridge_x_2b
-	9	-	9	-	9	-	9	-	11	Pilha 3	bridge_x_3a
10	-	10	-	10	-	10	-	14	-	bridge_x_4b	-
10	-	10	-	10	-	10	-	14	Empilha y	bridge_x_ya	11

-	11	-	11	-	11	-	15	-	ponte_x_yb	-	11

Configurações usando o FibreBridge 7500N ou 7600N usando apenas uma porta FC (FC1 ou FC2)									
GRUPO DE RD 2									
		Brocade G720		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520	
Pilha 1	bridge_x_51a	32	-	26	-	32	-	56	-
bridge_x_51b	-	32	-	26	-	32	-	56	Pilha 2
bridge_x_52a	33	-	27	-	33	-	57	-	bridge_x_52b
-	33	-	27	-	33	-	57	Pilha 3	bridge_x_53a
34	-	30	-	34	-	58	-	bridge_x_54b	-
34	-	30	-	34	-	58	Empilhay	bridge_x_ya	35
-	31	-	35	-	59	-	ponte_x_yb	-	35

14. Se você estiver configurando um sistema MetroCluster conetado em ponte, faça o cabeamento de cada ponte aos módulos do controlador:
    a. Cabo FC porta 1 da ponte para uma porta FC de 16 GB ou 8 GB no módulo do controlador em cluster_A.
    b. Cabo FC porta 2 da ponte para a mesma porta FC de velocidade do módulo do controlador em cluster_A.
    c. Repita esses subpassos em outras pontes subsequentes até que todas as pontes tenham sido cabeadas.
15. Atualize o firmware da unidade de disco para a versão mais atual a partir da consola do sistema:

    ```
    disk_fw_update
    ```

    Você deve executar este comando em ambos os módulos do controlador.

    "Downloads do NetApp: Firmware da unidade de disco"

16. Atualize o firmware do compartimento de disco para a versão mais atual usando as instruções para o firmware baixado.

    Você pode executar os comandos no procedimento a partir do console do sistema de qualquer módulo do controlador.

    "Downloads do NetApp: Firmware da gaveta de disco"

17. Se o sistema não tiver a atribuição automática de disco ativada, atribua a propriedade da unidade de disco.

    "Gerenciamento de disco e agregado"

    Se você estiver dividindo a propriedade de uma única pilha de compartimentos de disco entre vários módulos de controladora, será necessário desativar a atribuição automática de disco em ambos os nós no cluster (`storage disk option modify -autoassign off *`) antes de atribuir a propriedade de disco; caso contrário, quando você atribuir qualquer unidade de disco única, as unidades de disco restantes podem ser atribuídas automaticamente ao mesmo módulo e pool de controladora.

    Não é possível adicionar unidades de disco a agregados ou volumes até que o firmware da unidade de disco e do compartimento de disco tenham sido atualizados e as etapas de verificação nesta tarefa tenham sido concluídas.

18. Ative as portas do switch para a nova pilha.
19. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed
       `node run -node *node-name* sysconfig -a`
    b. Verifique se há alertas de integridade em ambos os clusters
       `system health alert show`
    c. Confirme a configuração do MetroCluster e se o modo operacional está normal
       `metrocluster show`
    d. Execute uma verificação MetroCluster
       `metrocluster check run`
    e. Exibir os resultados da verificação MetroCluster
       `metrocluster check show`
    f. Verifique se existem alertas de estado nos interrutores (se presentes)
       `storage switch show`
    g. Execute o Config Advisor.

       "NetApp Downloads: Config Advisor"

    h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.
20. Se aplicável, repita este procedimento para o local do parceiro.

Informações relacionadas

"Gerenciamento na banda das pontes FC para SAS"

Preparação para gavetas de disco SAS hot-add

Preparar para adicionar um compartimento de disco SAS a quente envolve o download de documentos, bem como o firmware da unidade de disco e do compartimento de disco.

- Seu sistema deve ser uma configuração com suporte e ter uma versão com suporte do ONTAP.
- Todas as unidades de disco e compartimentos de disco no sistema devem estar executando a versão de firmware mais recente.

  Talvez você queira atualizar o firmware do disco e do compartimento em toda a configuração do MetroCluster antes de adicionar gavetas.

  "Atualize, reverta ou downgrade"

> Uma combinação de IOM12 módulos e IOM6 módulos é suportada dentro da mesma pilha se o sistema estiver executando uma versão suportada do ONTAP. Para determinar se a sua versão do ONTAP suporta a mistura de prateleiras, consulte o "Ferramenta de Matriz de interoperabilidade (IMT)". Se a sua versão do ONTAP não for suportada e você não puder atualizar ou fazer o downgrade dos módulos IOM na stack existente ou na nova gaveta que deve ser adicionada a uma combinação suportada de módulos IOM, você precisará fazer um dos seguintes procedimentos:

- Inicie uma nova pilha em uma nova porta SAS (se suportada pelo par de pontes).
- Inicie uma nova pilha em um par de pontes adicional.

Passos

1. Faça o download ou veja os seguintes documentos no site de suporte da NetApp:
   - "Ferramenta de Matriz de interoperabilidade do NetApp"
   - O *Installation Guide* para o modelo do seu compartimento de disco.
2. Verifique se o compartimento de disco que você está adicionando a quente é suportado.

   "Ferramenta de Matriz de interoperabilidade do NetApp"

3. Transfira o firmware mais recente do compartimento de disco e disco:

> Nesta etapa, você só está completando a parte de download das instruções fornecidas nos links. Você precisa seguir as etapas encontradas na "Adição automática de um compartimento de disco"seção para instalar o compartimento de disco.

   a. Faça download do firmware do disco e faça uma cópia das instruções de firmware do disco para referência posterior.

      "Downloads do NetApp: Firmware da unidade de disco"

   b. Faça download do firmware do compartimento de disco e faça uma cópia das instruções de firmware do compartimento de disco para referência posteriormente.

      "Downloads do NetApp: Firmware da gaveta de disco"

Adição automática de um compartimento de disco

É possível adicionar um compartimento de disco a quente quando quiser aumentar o storage sem reduzir a performance.

- O sistema deve satisfazer todos os requisitos da "Preparação para gavetas de disco SAS hot-add".
- Para adicionar uma gaveta a quente, seu ambiente precisa atender a um dos cenários a seguir:
  - Você tem duas pontes do FibreBridge 7500N conetadas a uma pilha de gavetas de disco SAS.
  - Você tem duas pontes do FibreBridge 7600N conetadas a uma pilha de gavetas de disco SAS.
  - Você tem uma ponte FibreBridge 7500N e uma ponte FibreBridge 7600N conetada a uma pilha de gavetas de disco SAS.
- Esse procedimento serve para adicionar um compartimento de disco à última gaveta de disco em uma pilha.

  Este procedimento é escrito com o pressuposto de que o último compartimento de disco em uma stack está conetado da IOM A à ponte A e da IOM B à ponte B.
- Este é um procedimento sem interrupções.
- Você deve adicionar um número igual de compartimentos de disco em cada local.
- Se você estiver adicionando mais de um compartimento de disco, adicione um compartimento de disco de cada vez.

  Cada par de pontes FibreBridge 7500N ou 7600N pode suportar até quatro pilhas.

Adicionar um compartimento de disco requer que você atualize o firmware da unidade de disco no compartimento de disco hot-added executando o `storage disk firmware update` comando no modo avançado. A execução deste comando pode causar interrupções se o firmware nas unidades de disco existentes no seu sistema for uma versão mais antiga.

Se você inserir um cabo SAS na porta errada, ao remover o cabo de uma porta SAS, deverá aguardar pelo menos 120 segundos antes de conetar o cabo a uma porta SAS diferente. Se não o fizer, o sistema não reconhecerá que o cabo foi movido para outra porta.

Passos

1. Aterre-se corretamente.
2. Verifique a conectividade do compartimento de disco a partir do console do sistema de qualquer controlador:

   `sysconfig -v`

   A saída é semelhante ao seguinte:

   - Cada ponte em uma linha separada e sob cada porta FC à qual ela é visível; por exemplo, adicionar um compartimento de disco a um conjunto de bridgeBridge 7500N resulta na seguinte saída:

```
FC-to-SAS Bridge:
cisco_A_1-1:9.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100189
cisco_A_1-2:1.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100162
```

- Cada compartimento de disco em uma linha separada sob cada porta FC à qual ele é visível:

```
Shelf   0: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
Shelf   1: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
```

- Cada unidade de disco em uma linha separada sob cada porta FC para a qual ela é visível:

```
cisco_A_1-1:9.126L1   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
cisco_A_1-1:9.126L2   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
```

3. Verifique se o sistema tem atribuição automática de disco ativada a partir do console de qualquer controlador:

   `storage disk option show`

   A política de atribuição automática é mostrada na coluna atribuição automática.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

4. Se o sistema não tiver atribuição automática de disco ativada ou se as unidades de disco na mesma pilha forem de propriedade de ambos os controladores, atribua unidades de disco aos pools apropriados.

   "Gerenciamento de disco e agregado"

   Se você estiver dividindo uma única pilha de compartimentos de disco entre duas controladoras, a atribuição automática de disco deve ser desativada antes de atribuir a propriedade de disco; caso contrário, quando você atribuir qualquer unidade de disco única, as unidades de disco restantes podem ser atribuídas automaticamente ao mesmo controlador e pool.

   `storage disk option modify -node _node-name_ -autoassign off`O comando desativa a atribuição automática do disco.

As unidades de disco não devem ser adicionadas a agregados ou volumes até que o firmware da unidade de disco e do compartimento de disco tenham sido atualizados.

5. Atualize o firmware do compartimento de disco para a versão mais atual usando as instruções para o firmware baixado.

   Você pode executar os comandos no procedimento a partir do console do sistema de qualquer controlador.

   "Downloads do NetApp: Firmware da gaveta de disco"

6. Instale e faça o cabo da prateleira de discos:

   Não force um conetor para uma porta. Os cabos mini-SAS são chaveados; quando orientados corretamente para uma porta SAS, o cabo SAS clica no lugar e o LED LNK da porta SAS da gaveta de disco acende-se a verde.para as prateleiras de disco, você insere um conetor de cabo SAS com a aba de puxar orientada para cima (na parte superior do conetor).

   a. Instale o compartimento de disco, ligue-o e defina a ID do compartimento.

      O *Installation Guide* do modelo de compartimento de disco fornece informações detalhadas sobre a instalação das gavetas de disco.

      É necessário desligar o compartimento de disco e manter as IDs das gavetas exclusivas para cada compartimento de disco SAS em todo o sistema de storage.

   b. Desconete o cabo SAS da porta IOM B da última gaveta da stack e reconete-o à mesma porta da nova gaveta.

      A outra extremidade deste cabo permanece ligada à ponte B..

   c. Encadeie em série a nova gaveta de disco fazendo o cabeamento das novas portas IOM de gaveta (de Iom A e IOM B) até as últimas portas IOM de gaveta (de Iom A e IOM B).

   O *Installation Guide* para o modelo do seu compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.

7. Atualize o firmware da unidade de disco para a versão mais atual a partir da consola do sistema.

   "Downloads do NetApp: Firmware da unidade de disco"

   a. Mude para o nível de privilégio avançado
      `set -privilege advanced`

      Você precisa responder com **`y`** quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   b. Atualize o firmware da unidade de disco para a versão mais atual a partir da consola do sistema
      `storage disk firmware update`

   c. Voltar para o nível de privilégio de administrador
      `set -privilege admin`

d. Repita as subetapas anteriores no outro controlador.

8. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      node run -node *node-name* sysconfig -a

   b. Verifique se há alertas de integridade em ambos os clusters
      system health alert show
   c. Confirme a configuração do MetroCluster e se o modo operacional está normal
      metrocluster show
   d. Execute uma verificação MetroCluster
      metrocluster check run
   e. Apresentar os resultados da verificação MetroCluster:

      metrocluster check show

   f. Verifique se existem alertas de estado nos interrutores (se presentes):

      storage switch show

   g. Execute o Config Advisor.

      "NetApp Downloads: Config Advisor"

   h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.
9. Se você estiver adicionando mais de um compartimento de disco a quente, repita as etapas anteriores para cada compartimento de disco que você está adicionando a quente.

Adição automática de um compartimento de disco de IOM12 TB a uma stack de IOM6 shelves de disco em uma configuração MetroCluster conetada a uma ponte

Dependendo da sua versão do ONTAP, é possível adicionar um compartimento de disco de IOM12 TB a uma pilha de IOM6 compartimentos de disco em uma configuração MetroCluster conetada a uma ponte.

Para executar este procedimento, "Gavetas de adição dinâmica com IOM12 módulos para uma stack de gavetas com IOM6 módulos"consulte .

Storage com remoção automática de uma configuração MetroCluster FC

Você pode remover dinamicamente as gavetas de unidade — remover fisicamente as gavetas que tiveram os agregados removidos das unidades — de uma configuração de MetroCluster FC que está funcionando e fornecendo dados. É possível remover uma ou mais gavetas de qualquer lugar dentro de uma stack de gavetas ou remover uma stack de gavetas.

- Seu sistema precisa ser uma configuração de HA, multipath, HA de quatro caminhos ou de quatro caminhos.

- Em uma configuração de FC MetroCluster de quatro nós, o par de HA local não pode estar no estado de takeover.
- Você já deve ter removido todos os agregados das unidades nas gavetas que está removendo.

> Se você tentar este procedimento em configurações de FC que não são MetroCluster com agregados na gaveta que você está removendo, poderá fazer com que o sistema falhe em pânico de várias unidades.

A remoção de agregados envolve a divisão dos agregados espelhados nas gavetas que você está removendo e, em seguida, recriar os agregados espelhados com outro conjunto de unidades.

"Gerenciamento de disco e agregado"

- Você precisa ter removido a propriedade da unidade depois de remover os agregados das unidades nas gavetas que você está removendo.

"Gerenciamento de disco e agregado"

- Se você estiver removendo uma ou mais prateleiras de dentro de uma pilha, você deve ter fatorado a distância para ignorar as prateleiras que você está removendo.

Se os cabos atuais não forem longos o suficiente, você precisa ter cabos mais longos disponíveis.

Esta tarefa aplica-se às seguintes configurações do MetroCluster FC:

- Configurações de FC MetroCluster com conexão direta, nas quais os compartimentos de storage são conectados diretamente aos controladores de storage com cabos SAS
- Configurações de MetroCluster FC conectadas à malha ou em ponte, nas quais os compartimentos de storage são conectados por meio de pontes FC para SAS

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed
   node run -node *node-name* sysconfig -a
   b. Verifique se há alertas de integridade em ambos os clusters:

   system health alert show

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal
   metrocluster show
   d. Execute uma verificação MetroCluster:

   metrocluster check run

   e. Apresentar os resultados da verificação MetroCluster:

   metrocluster check show

   f. Verifique se existem alertas de estado nos interrutores (se presentes):

   storage switch show

g. Execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

2. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

3. Verifique se nenhuma unidade de caixa de correio está nas gavetas:
   `storage failover mailbox-disk show`

4. Retire a prateleira de acordo com as etapas para o cenário relevante.

Cenário	Passos
Para remover um agregado quando o shelf contém sem espelhamento, espelhado ou ambos os tipos de agregado…	a. Use o `storage aggregate delete -aggregate` *`aggregate name`* comando para remover o agregado. b. Use o procedimento padrão para remover a propriedade de todas as unidades nesse compartimento e, em seguida, remover fisicamente a gaveta. Siga as instruções no *SAS Disk Shelves Service Guide* para o modelo de prateleira para remover as prateleiras a quente.

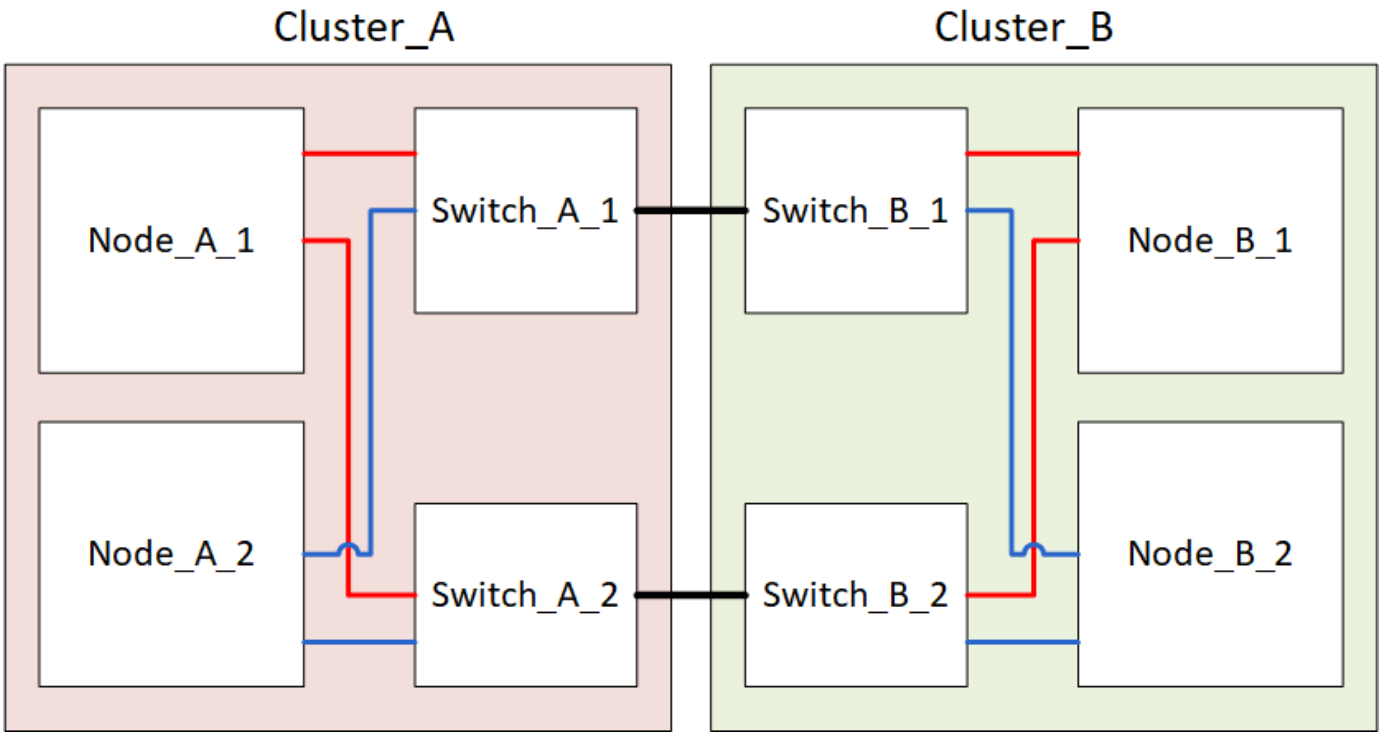
Para remover um Plex de um agregado espelhado, você precisa desespelhar o agregado.	a. Identifique o Plex que pretende remover utilizando o `run -node local sysconfig -r` comando. No exemplo a seguir, você pode identificar o Plex a partir da linha `Plex /dpg_mcc_8020_13_a1_aggr1/plex0`. Neste caso, o Plex a especificar é ""plex0"". `dpgmcc_8020_13_a1a2::storage aggregate> run -node local sysconfig -r` `*** This system has taken over dpg-mcc-8020-13-a1` `Aggregate dpg_mcc_8020_13_a1_aggr1 (online, raid_dp, mirrored) (block checksums)` `  Plex /dpg_mcc_8020_13_a1_aggr1/plex0 (online, normal, active, pool0)` `    RAID group /dpg_mcc_8020_13_a1_aggr1/plex0/rg0 (normal, block checksums)` `      RAID Disk Device HA  SHELF BAY CHAN Pool Type RPM  Used (MB/blks)    Phys (MB/blks)` `      --------- ------ ------------- ---- ---- ---- ----- -------------- --------------` `      dparity   mcc-cisco-8Gb-fab-2:1-1.126L16  0c    32  15 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      parity    mcc-cisco-8Gb-fab-2:1-1.126L18  0c    32  17 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      data      mcc-cisco-8Gb-fab-2:1-1.126L19  0c    32  18 FC:B   0   SAS 15000 272000/557056000 274845/562884296` `      data      mcc-cisco-8Gb-`

Desligue e ligue um único local em uma configuração MetroCluster FC

Se você precisar executar a manutenção do local ou realocar um único local em uma configuração do MetroCluster FC, você deve saber como desligar e ligar o local.

Se você precisar realocar e reconfigurar um local (por exemplo, se precisar expandir de um cluster de quatro nós para um cluster de oito nós), não será possível concluir essas tarefas ao mesmo tempo. Este procedimento abrange apenas as etapas necessárias para realizar a manutenção do local ou para realocar um local sem alterar sua configuração.

O diagrama a seguir mostra uma configuração do MetroCluster. Cluster_B está desligado para manutenção.



Desligue um site da MetroCluster

Você deve desligar um local e todo o equipamento antes que a manutenção ou realocação do local possa começar.

Sobre esta tarefa

Todos os comandos nas etapas a seguir são emitidos a partir do site que permanece ligado.

Passos

1. Antes de começar, verifique se todos os agregados não espelhados no site estão offline.
2. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verifique se há alertas de integridade em ambos os clusters:

      ```
      system health alert show
      ```

```
fab-3:1-1.126L21   0c    32  20
FC:B   0   SAS 15000
272000/557056000
274845/562884296
      data      mcc-cisco-8Gb-
fab-3:1-1.126L22   0c    32  21
FC:B   0   SAS 15000
272000/557056000
274845/562884296
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      parity    mcc-cisco-8Gb-
fab-3:1-1.126L14   0d    33  13
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L41   0d    34  14
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L15   0d    33  14
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L45   0d    34  18
```

c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

```
metrocluster show
```

d. Execute uma verificação MetroCluster
`metrocluster check run`

e. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

f. Verifique se existem alertas de estado nos interrutores (se presentes):

```
storage switch show
```

g. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

```
FC:A   1   SAS 15000
       272000/557056000
       280104/573653840
```

b. Utilizar o `storage aggregate plex delete -aggregate aggr_name -plex plex_name` comando para extrair o Plex.

plex define o nome do plex, como "'plex3" ou "'plex6".

c. Use o procedimento padrão para remover a propriedade de todas as unidades nesse compartimento e, em seguida, remover fisicamente a gaveta.

Siga as instruções no *SAS Disk Shelves Service Guide* para o modelo de prateleira para remover as prateleiras a quente.

3. A partir do local em que você deseja permanecer ativo, implemente o switchover:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

A operação pode levar vários minutos para ser concluída.

Os agregados sem espelhamento só estarão online após um switchover se os discos remotos no agregado estiverem acessíveis. Se os ISLs falharem, o nó local poderá não conseguir aceder aos dados nos discos remotos sem espelhamento. A falha de um agregado pode levar a uma reinicialização do nó local.

4. Monitorize e verifique a conclusão do switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Mova todos os volumes e LUNs que pertençam a agregados sem espelhamento offline.
   a. Mova os volumes offline.

      ```
      cluster_A::* volume offline <volume name>
      ```

   b. Mova os LUNs off-line.

      ```
      cluster_A::* lun offline lun_path <lun_path>
      ```

6. Mover agregados sem espelhamento offline: `storage aggregate offline`

   ```
   cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
   ```

7. Dependendo da configuração e da versão do ONTAP, identifique e mova os plexos afetados offline que estão localizados no local de desastre (Cluster_B).

   Você deve mover os seguintes plexes off-line:

   - Plexos não espelhados residentes em discos localizados no local de desastre.

     Se você não mover os plexos não espelhados no local de desastre off-line, uma interrupção pode ocorrer quando o local de desastre for desligado mais tarde.

   - Plexos espelhados que residem em discos localizados no local de desastre para espelhamento agregado. Depois que eles são movidos off-line, os plexes são inacessíveis.

   a. Identificar os plexos afetados.

      Os plexes que são propriedade de nós no local sobrevivente consistem em Pool1 discos. Os plexes que são propriedade de nós no local de desastre consistem em Pool0 discos.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

Os plexos afetados são aqueles que são remotos para o cluster A. a tabela a seguir mostra se os discos são locais ou remotos em relação ao cluster A:

Nó	Discos no pool	Os discos devem ser configurados offline?	Exemplo de plexes a serem movidos off-line
Nó _A_1 e nó _A_2	Discos no pool 0	Os discos não são locais para o cluster A..	-
Discos no pool 1	Sim. Os discos são remotos para o cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nó _B_1 e nó _B_2

Discos no pool 0	Sim. Os discos são remotos para o cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Discos no pool 1

b. Mova os plexes afetados offline:

`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

Execute esta etapa para todos os plexos que têm discos remotos para Cluster_A.

8. Persistentemente offline as portas do switch ISL de acordo com o tipo de switch.

Tipo de interrutor	Ação

Para switches Brocade FC…	a. Use o `portcfgpersistentdisable <port>` comando para desativar persistentemente as portas como mostrado no exemplo a seguir. Isso deve ser feito em ambos os switches no local sobrevivente. `Switch_A_1:admin> portcfgpersistentdisable 14` `Switch_A_1:admin> portcfgpersistentdisable 15` `Switch_A_1:admin>` b. Verifique se as portas estão desativadas usando o `switchshow` comando mostrado no exemplo a seguir: `Switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G No_Light FC` `Disabled (Persistent)` `15 15 020f00 id 16G No_Light FC` `Disabled (Persistent)` `...` `Switch_A_1:admin>`

Para switches Cisco FC…	a. Use o `interface` comando para desativar persistentemente as portas. O exemplo a seguir mostra as portas 14 e 15 sendo desativadas: `Switch_A_1# conf t` `Switch_A_1(config)# interface fc1/14-15` `Switch_A_1(config)# shut` `Switch_A_1(config-if)# end` `Switch_A_1# copy running-config startup-config` b. Verifique se a porta do switch está desativada usando o `show interface brief` comando, conforme mostrado no exemplo a seguir: `Switch_A_1# show interface brief` `Switch_A_1`

9. Desligue o equipamento no local do desastre.

   O seguinte equipamento deve ser desligado pela ordem indicada:

   - Controladores de armazenamento - os controladores de armazenamento devem estar `LOADER` no prompt, você deve desligá-los completamente.
   - Switches MetroCluster FC
   - ATTO FibreBridges (se presente)
   - Prateleiras de storage

Mudar o local desligado do MetroCluster

Depois de o site ser desligado, você pode começar o trabalho de manutenção. O procedimento é o mesmo se os componentes do MetroCluster forem relocados no mesmo data center ou relocados para um data center diferente.

- O hardware deve ser cabeado da mesma forma que o site anterior.
- Se a velocidade, o comprimento ou o número do enlace inter-switch (ISL) tiverem sido alterados, todos eles precisam ser reconfigurados.

Passos

1. Verifique se o cabeamento de todos os componentes é cuidadosamente gravado para que ele possa ser reconetado corretamente no novo local.
2. Realocar fisicamente todo o hardware, controladores de storage, switches FC, FibreBridges e compartimentos de storage.
3. Configure as portas ISL e verifique a conetividade entre sites.

   a. Ligue os switches FC.

Não ligue nenhum outro equipamento.

b. Ative as portas.

Ative as portas de acordo com os tipos de switch corretos na seguinte tabela:

Tipo de interrutor	Comando

Para switches Brocade FC…	i. Use o `portcfgpersistentenable <port number>` comando para ativar persistentemente a porta. Isso deve ser feito em ambos os switches no local sobrevivente. O exemplo a seguir mostra as portas 14 e 15 sendo ativadas no Switch_A_1. ``` switch_A_1:admin> portcfgpersistentenable 14 switch_A_1:admin> portcfgpersistentenable 15 switch_A_1:admin> ``` ii. Verifique se a porta do switch está ativada: `switchshow` O exemplo a seguir mostra que as portas 14 e 15 estão ativadas: ``` switch_A_1:admin> switchshow switchName: Switch_A_1 switchType: 109.1 switchState: Online switchMode: Native switchRole: Principal switchDomain: 2 switchId: fffc02 switchWwn: 10:00:00:05:33:88:9c:68 zoning: ON (T5_T6) switchBeacon: OFF FC Router: OFF FC Router BB Fabric ID: 128 Address Mode: 0 Index Port Address Media Speed State Proto == ==== ... 14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" 15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream) ... switch_A_1:admin> ```

Para switches Cisco FC…	i. Digite o `interface` comando para ativar a porta. O exemplo a seguir mostra as portas 14 e 15 sendo ativadas no Switch_A_1. ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# no shut switch_A_1(config-if)# end switch_A_1# copy running-config startup-config ``` ii. Verifique se a porta do switch está ativada: `show interface brief` ``` switch_A_1# show interface brief switch_A_1# ```

4. Use ferramentas nos switches (conforme disponíveis) para verificar a conetividade entre sites.

   Você só deve prosseguir se os links estiverem corretamente configurados e estáveis.

5. Desative os links novamente se eles forem encontrados estáveis.

   Desative as portas com base se você está usando switches Brocade ou Cisco, conforme mostrado na tabela a seguir:

Tipo de interrutor	Comando

Para switches Brocade FC…	a. Digite o `portcfgpersistentdisable <port_number>` comando para desativar persistentemente a porta. Isso deve ser feito em ambos os switches no local sobrevivente. O exemplo a seguir mostra as portas 14 e 15 sendo desativadas no Switch_A_1: `switch_A_1:admin> portpersistentdisable 14` `switch_A_1:admin> portpersistentdisable 15` `switch_A_1:admin>` b. Verifique se a porta do switch está desativada: `switchshow` O exemplo a seguir mostra que as portas 14 e 15 estão desativadas: `switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G No_Light FC Disabled (Persistent)` `15 15 020f00 id 16G No_Light FC Disabled (Persistent)` `...` `switch_A_1:admin>`

Para switches Cisco FC…	a. Desative a porta usando o `interface` comando. O exemplo a seguir mostra que as portas FC1/14 e FC1/15 estão sendo desativadas no interrutor A_1: `switch_A_1# conf t` `switch_A_1(config)# interface fc1/14-15` `switch_A_1(config)# shut` `switch_A_1(config-if)# end` `switch_A_1# copy running-config startup-config` b. Verifique se a porta do switch está desativada usando o `show interface brief` comando. `switch_A_1# show interface brief` `switch_A_1#`

Ligar a configuração do MetroCluster e regressar ao funcionamento normal

Após a manutenção ter sido concluída ou o site ter sido movido, você deve ligar o site e restabelecer a configuração do MetroCluster.

Sobre esta tarefa

Todos os comandos nas etapas a seguir são emitidos a partir do site em que você liga.

Passos

1. Ligue os interrutores.

   Deve ligar primeiro os interrutores. Eles podem ter sido ligados durante a etapa anterior se o local foi transferido.

   a. Reconfigure a ligação entre interrutores (ISL), se necessário, ou se esta não tiver sido concluída como parte da realocação.
   b. Ative o ISL se a vedação tiver sido concluída.
   c. Verifique o ISL.
2. Desative os ISLs nos switches FC.
3. Ligue as prateleiras e deixe tempo suficiente para que elas se liguem completamente.
4. Ligue as pontes FibreBridge.
   a. Nos switches FC, verifique se as portas que conetam as pontes estão sendo conetadas.

      Você pode usar um comando como `switchshow` para switches Brocade e `show interface brief` para switches Cisco.

b. Verifique se as prateleiras e os discos nas pontes estão claramente visíveis.

   Você pode usar um comando como `sastargets` no ATTO CLI.

5. Ative os ISLs nos switches FC.

   Ative as portas com base se você está usando switches Brocade ou Cisco, conforme mostrado na tabela a seguir:

Tipo de interrutor	Comando

Para switches Brocade FC…	a. Digite o `portcfgpersistentenable <port>` comando para ativar persistentemente as portas. Isso deve ser feito em ambos os switches no local sobrevivente. O exemplo a seguir mostra as portas 14 e 15 sendo ativadas no Switch_A_1: `Switch_A_1:admin> portcfgpersistentenable 14` `Switch_A_1:admin> portcfgpersistentenable 15` `Switch_A_1:admin>` b. Verifique se a porta do switch está ativada usando o comando mais `switchshow`: `switch_A_1:admin> switchshow` `switchName: Switch_A_1` `switchType: 109.1` `switchState: Online` `switchMode: Native` `switchRole: Principal` `switchDomain: 2` `switchId: fffc02` `switchWwn: 10:00:00:05:33:88:9c:68` `zoning: ON (T5_T6)` `switchBeacon: OFF` `FC Router: OFF` `FC Router BB Fabric ID: 128` `Address Mode: 0` `Index Port Address Media Speed State Proto` `==========` `...` `14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1"` `15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)` `...` `switch_A_1:admin>`

Para switches Cisco FC…	a. Use o `interface` comando para ativar as portas. O exemplo a seguir mostra a porta FC1/14 e FC1/15 sendo ativada no interrutor A_1: ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# no shut switch_A_1(config-if)# end switch_A_1# copy running-config startup-config ``` b. Verifique se a porta do switch está desativada: ``` switch_A_1# show interface brief switch_A_1# ```

6. Verifique se o armazenamento está visível.
   a. Verifique se o armazenamento está visível a partir do local sobrevivente. Coloque os plexes offline novamente online para reiniciar a operação ressincronizada e restabelecer o SyncMirror.
   b. Verifique se o armazenamento local está visível a partir do nó no modo Manutenção:

      ```
      disk show -v
      ```

7. Restabelecer a configuração do MetroCluster.

   Siga as instruções em "Verificando se o sistema está pronto para um switchback" para executar operações de recuperação e switchback de acordo com sua configuração do MetroCluster.

Desativar toda uma configuração do MetroCluster FC

Você precisa desligar toda a configuração do MetroCluster FC e todos os equipamentos antes que a manutenção ou realocação do local possa começar.

Sobre esta tarefa

Tem de executar as etapas deste procedimento a partir de ambos os locais, ao mesmo tempo.

> A partir de ONTAP 9.8, o **`storage switch`** comando é substituído por **`system switch`**. As etapas a seguir mostram o **`storage switch`** comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o **`system switch`** comando é preferido.

Passos

1. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal. E **`metrocluster show`**

b. Confirme a conetividade com os discos inserindo o seguinte comando em qualquer um dos nós MetroCluster
run local sysconfig -v

c. Execute o seguinte comando
storage bridge show

d. Execute o seguinte comando
storage port show

e. Execute o seguinte comando
storage switch show

f. Execute o seguinte comando
network port show

g. Execute uma verificação MetroCluster
metrocluster check run

h. Exibir os resultados da verificação MetroCluster
metrocluster check show

2. Desative o AUSO modificando o domínio de falha do AUSO para

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

3. Verifique a alteração usando o comando

metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Interrompa os nós usando o seguinte comando:
halt

◦ Para uma configuração de MetroCluster de quatro ou oito nós, use os **inhibit-takeover** parâmetros e **skip-lif-migration-before-shutdown**:

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore
-quorum-warnings true -skip-lif-migration-before-shutdown true
```

◦ Para uma configuração MetroCluster de dois nós, use o comando:

```
system node halt -node node1_SiteA -ignore-quorum-warnings true
```

5. Desligue o seguinte equipamento no local:
   - Controladores de storage
   - Switches MetroCluster FC (se em uso e a configuração não for uma configuração de alongamento de dois nós)
   - ATTO FibreBridges
   - Prateleiras de storage
6. Aguarde trinta minutos e, em seguida, ligue o seguinte equipamento no local:
   - Prateleiras de storage
   - ATTO FibreBridges
   - Switches MetroCluster FC
   - Controladores de storage
7. Depois que os controladores estiverem ligados, verifique a configuração do MetroCluster de ambos os sites.

   Para verificar a configuração, repita a etapa 1.

8. Execute as verificações do ciclo de alimentação.
   a. Verifique se todas as SVMs de origem sincronizada estão online
   `vserver show`
   b. Inicie qualquer SVMs de origem sincronizada que não estejam online
   `vserver start`

Procedimentos de manutenção para configurações IP do MetroCluster

Modifique as propriedades de uma interface IP do MetroCluster

A partir do ONTAP 9.10,1, você pode alterar as seguintes propriedades de uma interface IP MetroCluster: Endereço IP e máscara e gateway. Você pode usar qualquer combinação de parâmetros para atualizar.

Talvez seja necessário atualizar essas propriedades, por exemplo, se um endereço IP duplicado for detetado ou se um gateway precisar mudar no caso de uma rede de camada 3 devido a alterações na configuração do roteador.

Modifique o endereço IP, a máscara de rede e o gateway

O procedimento a seguir depende se você está usando o Gerenciador de sistema do ONTAP ou a CLI.

System Manager

Use o System Manager para modificar o endereço IP, a máscara de rede e as propriedades do gateway.

Passo

Atualize o endereço IP, a máscara de rede e o gateway para cada nó e interface.

CLI

Use a CLI para modificar o endereço IP, a máscara de rede e as propriedades do gateway.

Sobre esta tarefa

- Você só pode alterar uma interface de cada vez. Haverá interrupção de tráfego nessa interface até que as outras interfaces sejam atualizadas e as conexões sejam restabelecidas.
- Use o `metrocluster configuration-settings interface modify` comando para alterar qualquer propriedade da interface IP do MetroCluster.

> Esses comandos alteram a configuração em um nó específico para uma porta específica. Para restaurar a conetividade de rede completa, comandos semelhantes são necessários em outras portas. Da mesma forma, os switches de rede também precisam atualizar sua configuração. Por exemplo, se o gateway for atualizado, o ideal é que ele seja alterado em ambos os nós de um par de HA, já que eles são os mesmos. O switch conetado a esses nós também precisa atualizar seu gateway.

- Use os `metrocluster configuration-settings interface show` comandos , `metrocluster connection check` e `metrocluster connection show` para verificar se toda a conetividade está funcionando em todas as interfaces.

Passos

1. Atualize o endereço IP, a máscara de rede e o gateway para um único nó e interface: `metrocluster configuration-settings interface modify`

   O comando a seguir mostra como atualizar o endereço IP, a máscara de rede e o gateway:

```
cluster_A::* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10
-address 192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner
nodes may need modifications for port "e0a-10" in order to
completely establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsi13:0:-
1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsi14:0:-1:0): xpt_action_default: CCB type 0xe
XPT_DEV_ADVINFO not supported
(pass8:iscsi15:0:-1:0): xpt_action_default: CCB type 0xe
XPT_DEV_ADVINFO not supported
(pass9:iscsi16:0:-1:0): xpt_action_default: CCB type 0xe
XPT_DEV_ADVINFO not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10
-address 192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner
nodes may need modifications for port "e0a-10" in order to
completely establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful
```

2. Verifique se toda a conetividade está funcionando para todas as interfaces:
`metrocluster configuration-settings interface show`

   O comando a seguir mostra como verificar se toda a conetividade está funcionando para todas as interfaces:

```
cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR              Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- ---------------
--------------- ---------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.12.201  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.200  255.255.255.0   192.168.20.1
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.12.101  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.101  255.255.255.0   192.168.20.1
completed
      cluster_B node_B_1
                 Home Port: e0a-10
                      192.168.11.151  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.150  255.255.255.0   192.168.21.1
completed
                node_B_2
                 Home Port: e0a-10
                      192.168.11.250  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.250  255.255.255.0   192.168.21.1
completed
8 entries were displayed.
```

3. Verifique se todas as conexões estão funcionando:

   `metrocluster configuration-settings connection show`

   O comando a seguir mostra como verificar se todas as conexões estão funcionando:

```
cluster_A::*> metrocluster configuration-settings connection show
  (metrocluster configuration-settings connection show)
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A node_A_2
                  Home Port: e0a-10
                       192.168.10.200  192.168.10.101  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.250  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.151  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.20.100  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.250  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.150  DR Auxiliary
completed
                 node_A_1
                  Home Port: e0a-10
                       192.168.10.101  192.168.10.200  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.151  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.250  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.20.200  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.150  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.250  DR Auxiliary
completed
```

Manutenção e substituição do interrutor IP

Substitua um switch IP ou altere o uso de switches IP MetroCluster existentes

Talvez seja necessário substituir um switch com falha, atualizar ou fazer downgrade de um switch ou alterar o uso de switches IP MetroCluster existentes.

Sobre esta tarefa

Este procedimento aplica-se quando você está usando switches validados pela NetApp. Se você estiver usando switches compatíveis com MetroCluster, consulte o fornecedor do switch.

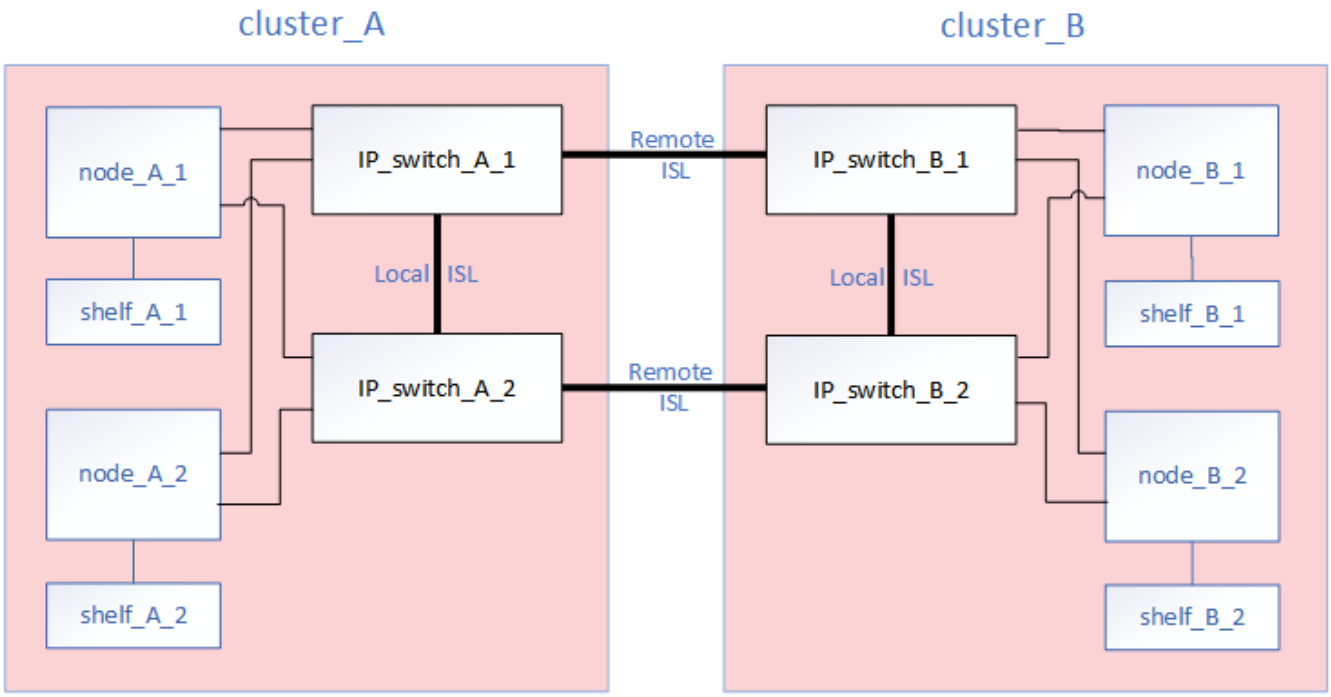
"Ativar o registo da consola" antes de executar esta tarefa.

Este procedimento suporta as seguintes conversões:

- Alterar o fornecedor, tipo ou ambos do switch. O novo switch pode ser o mesmo que o antigo switch quando um switch falhou, ou você pode alterar o tipo de switch (atualizar ou fazer downgrade do switch).

  Por exemplo, para expandir uma configuração IP MetroCluster de uma configuração de quatro nós usando controladores AFF A400 e switches BES-53248 para uma configuração de oito nós usando controladores AFF A400, você deve alterar os switches para um tipo compatível para a configuração, pois os switches BES-53248 não são suportados na nova configuração.

  Se você quiser substituir um switch com falha pelo mesmo tipo de switch, você só substitui o switch com falha. Se você quiser atualizar ou fazer downgrade de um switch, você deve ajustar dois switches que estão na mesma rede. Dois switches estão na mesma rede quando estão conetados com um link inter-switch (ISL) e não estão localizados no mesmo local. Por exemplo, a rede 1 inclui IP_switch_A_1 e IP_switch_B_1, e a rede 2 inclui IP_switch_A_2 e IP_switch_B_2, como mostrado no diagrama abaixo:



Se você substituir um switch ou atualizar para diferentes switches, poderá pré-configurar os switches instalando o firmware do switch e o arquivo RCF.

- Converta uma configuração IP MetroCluster para uma configuração IP MetroCluster usando switches MetroCluster de armazenamento compartilhado.

  Por exemplo, se você tiver uma configuração MetroCluster IP normal usando controladores AFF A700 e quiser reconfigurar o MetroCluster para conetar gavetas NS224 aos mesmos switches.

  - Se estiver adicionando ou removendo prateleiras em uma configuração MetroCluster IP usando switches IP MetroCluster de armazenamento compartilhado, siga as etapas em "Adição de gavetas a um IP MetroCluster usando switches MetroCluster de armazenamento compartilhado"
  - Sua configuração IP do MetroCluster pode já se conectar diretamente às gavetas NS224 ou a switches de storage dedicados.

Folha de cálculo de utilização de portas

A seguir está uma Planilha de exemplo para converter uma configuração IP do MetroCluster para uma configuração de armazenamento compartilhado conetando duas prateleiras NS224 usando os switches existentes.

Definições da folha de cálculo:

- Configuração existente: O cabeamento da configuração MetroCluster existente.
- Nova configuração com NS224 gavetas: A configuração de destino em que os switches são compartilhados entre o storage e o MetroCluster.

Os campos realçados nesta folha de trabalho indicam o seguinte:

- Verde: Você não precisa alterar o cabeamento.
- Amarelo: Você deve mover portas com a mesma configuração ou uma configuração diferente.
- Azul: Portas que são novas conexões.

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

Passos

1. Verifique a integridade da configuração.
   a. Verifique se o MetroCluster está configurado e no modo normal em cada cluster: **metrocluster show**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verifique se o espelhamento está ativado em cada nó: **metrocluster node show**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Verifique se os componentes do MetroCluster estão em bom estado: **metrocluster check run**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Verifique se não existem alertas de saúde: **`system health alert show`**

2. Configure o novo switch antes da instalação.

   Se estiver a reutilizar comutadores existentes, vá para Passo 4.

   > Se você estiver atualizando ou baixando os switches, deverá configurar todos os switches na rede.

   Siga as etapas na seção *Configurando os switches IP* no "Instalação e configuração IP do MetroCluster."

   Certifique-se de aplicar o arquivo RCF correto para o switch _A_1, _A_2, _B_1 ou _B_2. Se o novo switch for o mesmo que o antigo, você precisará aplicar o mesmo arquivo RCF.

   Se você atualizar ou baixar um switch, aplique o arquivo RCF mais recente suportado para o novo switch.

3. Execute o comando port show para exibir informações sobre as portas de rede:

   `network port show`

   a. Modifique todas as LIFs do cluster para desativar a reversão automática:

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. desligue as ligações do interrutor antigo.

Você só desconeta conexões que não estejam usando a mesma porta nas configurações antigas e novas. Se estiver a utilizar novos comutadores, tem de desligar todas as ligações.

Extrair as ligações pela seguinte ordem:

a. Desligue as interfaces do cluster local
b. Desligue as ISLs do cluster local
c. Desligue as interfaces IP do MetroCluster
d. Desligue os ISLs da MetroCluster

No exemplo [port_usage_worksheet], os interrutores não mudam. Os ISLs da MetroCluster são relocados e devem ser desconetados. Não é necessário desligar as ligações marcadas a verde na folha de trabalho.

5. Se você estiver usando novos switches, desligue o interrutor antigo, remova os cabos e remova fisicamente o interrutor antigo.

Se estiver a reutilizar comutadores existentes, vá para Passo 6.

Not cable os novos switches, exceto para a interface de gerenciamento (se usado).

6. Configure os switches existentes.

Se já tiver pré-configurado os parâmetros, pode ignorar este passo.

Para configurar os switches existentes, siga as etapas para instalar e atualizar os arquivos de firmware e RCF:

- "Atualizando o firmware em switches IP MetroCluster"
- "Atualize arquivos RCF em switches IP MetroCluster"

7. Coloque o cabo dos interrutores.

Você pode seguir as etapas na seção *cabeamento dos switches IP* no "Instalação e configuração IP do MetroCluster".

Ligue os interrutores pela seguinte ordem (se necessário):

a. Faça o cabo das ISLs para o local remoto.
b. Faça o cabo das interfaces IP do MetroCluster.
c. Faça o cabeamento das interfaces do cluster local.

- As portas usadas podem ser diferentes daquelas no switch antigo se o tipo de switch for diferente. Se você estiver atualizando ou baixando os switches, **NÃO** faça o cabo dos ISLs locais. Somente faça o cabeamento dos ISLs locais se você estiver atualizando ou baixando os switches na segunda rede e ambos os switches em um local forem do mesmo tipo e cabeamento.
- Se você estiver atualizando o Switch-A1 e o Switch-B1, execute as etapas 1 a 6 para os switches Switch-A2 e Switch-B2.

8. Finalizar o cabeamento do cluster local.

a. Se as interfaces de cluster locais estiverem conetadas a um switch:

   i. Faça o cabo das ISLs do cluster local.

b. Se as interfaces de cluster locais estiverem **não** conetadas a um switch:

   i. Use o "Migrar para um ambiente de cluster comutado do NetApp" procedimento para converter um cluster sem switch para um cluster comutado. Use as portas indicadas em "Instalação e configuração IP do MetroCluster" ou os arquivos de cabeamento RCF para conetar a interface do cluster local.

9. Ligue o interrutor ou os interrutores.

   Se o novo interrutor for o mesmo, ligue o novo interrutor. Se você estiver atualizando ou baixando os switches, então ligue os dois switches. A configuração pode operar com dois switches diferentes em cada local até que a segunda rede seja atualizada.

10. Verifique se a configuração do MetroCluster está saudável repetindo Passo 1.

    Se você estiver atualizando ou baixando os switches na primeira rede, poderá ver alguns alertas relacionados ao clustering local.

    Se você atualizar ou baixar as redes, repita todas as etapas da segunda rede.

11. Modifique todas as LIFs do cluster para reativar a reversão automática:

    ```
    network interface modify -vserver <vserver_name> -lif <lif_name> -auto
    -revert true
    ```

12. Opcionalmente, mova as NS224 gavetas.

    Se você estiver reconfigurando uma configuração IP do MetroCluster que não conete as gavetas NS224 aos switches IP do MetroCluster, use o procedimento apropriado para adicionar ou mover as gavetas NS224:

    - "Adição de gavetas a um IP MetroCluster usando switches MetroCluster de armazenamento compartilhado"
    - "Migre de um cluster sem switch com storage de conexão direta"
    - "Migre de uma configuração sem switch com storage conectado ao switch reutilizando os switches"

Portas de interface IP MetroCluster online ou offline

Quando você executa tarefas de manutenção, talvez seja necessário colocar uma porta de interface IP do MetroCluster offline ou online.

Sobre esta tarefa

"Ativar o registo da consola" antes de executar esta tarefa.

Passos

Você pode usar as etapas a seguir para colocar uma porta de interface IP do MetroCluster online ou colocá-la offline.

1. Defina o nível de privilégio como avançado.

```
set -privilege advanced
```

Exemplo de saída

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. Coloque a porta de interface IP do MetroCluster offline.

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

Exemplo de saída

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

a. Verifique se a interface IP do MetroCluster está offline.

```
Cluster_A1::*> system ha interconnect port show
```

Exemplo de saída

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1         off
                             0  disabled  down              4          3
false
                             1  linkup    active            4          2
true
node-a2         off
                             0  linkup    active            4          2
true
                             1  linkup    active            4          2
true
2 entries were displayed.
```

3. Coloque a porta de interface IP do MetroCluster online.

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

Exemplo de saída

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. Verifique se a porta de interface IP do MetroCluster está online.

```
Cluster_A1::*> system ha interconnect port show
```

Exemplo de saída

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  linkup    active            5          3
true
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

Atualizando o firmware em switches IP MetroCluster

Talvez seja necessário atualizar o firmware em um switch IP MetroCluster.

Sobre esta tarefa

Você deve repetir esta tarefa em cada uma das opções sucessivamente.

"Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Verifique a integridade da configuração.

   a. Verifique se o MetroCluster está configurado e no modo normal em cada cluster:

      ```
      metrocluster show
      ```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Verifique se o espelhamento está ativado em cada nó:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Verifique se os componentes do MetroCluster estão em bom estado:

`metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

a. Verifique se não existem alertas de saúde:

```
system health alert show
```

2. Instale o software no primeiro interrutor.

> Tem de instalar o software do interrutor nos interrutores pela seguinte ordem: Switch_A_1, switch_B_1, switch_A_2, switch_B_2.

Siga as etapas para instalar o software do switch no tópico relevante, dependendo se o tipo de switch é Broadcom, Cisco ou NVIDIA:

- "Baixe e instale o software Broadcom switch EFOS"
- "Baixe e instale o software Cisco switch NX-os"
- "Baixe e instale o software Cumulus switch NVIDIA SN2100"

3. Repita o passo anterior para cada um dos interrutores.
4. Repita Passo 1 para verificar a integridade da configuração.

Atualize arquivos RCF em switches IP MetroCluster

Talvez seja necessário atualizar um arquivo RCF em um switch IP MetroCluster. Por exemplo, se a versão do arquivo RCF que você está executando nos switches não for suportada pela versão do ONTAP, pela versão do firmware do switch ou por ambos.

Verifique se o arquivo RCF é suportado

Se você estiver alterando a versão do ONTAP ou a versão do firmware do switch, verifique se você tem um arquivo RCF compatível com essa versão. Se você usar o gerador RCF, o arquivo RCF correto será gerado para você.

Passos

1. Use os seguintes comandos dos switches para verificar a versão do arquivo RCF:

A partir deste interrutor…	Emitir este comando…
Interrutor Broadcom	`(IP_switch_A_1) # show clibanner`
Interrutor Cisco	`IP_switch_A_1# show banner motd`

   Para qualquer switch, localize a linha na saída que indica a versão do arquivo RCF. Por exemplo, a saída a seguir é de um switch Cisco, que indica que a versão do arquivo RCF é "'v1,80'".

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Para verificar quais arquivos são suportados para uma versão, switch e plataforma específica do ONTAP, use o RcfFileGenerator. Se você pode gerar o arquivo RCF para a configuração que você tem ou para a qual deseja atualizar, então ele é suportado.
3. Para verificar se o firmware do switch é suportado, consulte o seguinte:
   - "Hardware Universe"
   - "Matriz de interoperabilidade do NetApp"

Atualize arquivos RCF

Se você estiver instalando o novo firmware do switch, você deve instalar o firmware do switch antes de atualizar o arquivo RCF.

Sobre esta tarefa

- Este procedimento interrompe o tráfego no switch onde o arquivo RCF é atualizado. O tráfego será retomado quando o novo arquivo RCF for aplicado.
- Execute os passos em um interrutor de cada vez, na seguinte ordem: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.
- "Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Verifique a integridade da configuração.
   a. Verifique se os componentes do MetroCluster estão em bom estado:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

      A operação é executada em segundo plano.

   b. Após a `metrocluster check run` conclusão da operação, execute `metrocluster check show` para visualizar os resultados.

Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id 38
```

b. Verifique se não há alertas de saúde:

```
system health alert show
```

2. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"

3. Baixe e instale o arquivo RCF IP, dependendo do fornecedor do switch.
   - "Baixe e instale os arquivos Broadcom IP RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

> Se você tiver uma configuração de rede L2 compartilhada ou L3, talvez seja necessário ajustar as portas ISL nos switches intermediários/clientes. O modo switchport pode mudar do modo 'Access' para o modo 'trunk'. Apenas prossiga para atualizar o segundo par de switches (A_2, B_2) se a conetividade de rede entre os switches A_1 e B_1 estiver totalmente operacional e a rede estiver em bom estado.

Atualize arquivos RCF em switches IP Cisco usando CleanUpFiles

Talvez seja necessário atualizar um arquivo RCF em um switch IP Cisco. Por exemplo, uma atualização do ONTAP ou uma atualização do firmware do switch exigem um novo

arquivo RCF.

Sobre esta tarefa

- Começando com RcfFileGenerator versão 1,4a, há uma nova opção para alterar (atualizar, baixar ou substituir) a configuração do switch em switches IP Cisco sem a necessidade de executar uma 'eliminação de gravação'.
- "Ativar o registo da consola" antes de executar esta tarefa.
- O switch Cisco 9336C-FX2 tem dois tipos diferentes de armazenamento de switch que são nomeados de forma diferente no RCF. Use a tabela a seguir para determinar o tipo de armazenamento Cisco 9336C-FX2 correto para sua configuração:

Se estiver a ligar o seguinte armazenamento…	Escolha o tipo de armazenamento Cisco 9336C-FX2…	Exemplo de banner de arquivo RCF/MOTD
• Gavetas SAS conectadas diretamente • Gavetas NVMe diretamente conectadas • Gavetas NVMe conectadas a switches de storage dedicados	9336C-FX2 – apenas armazenamento direto	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• Gavetas SAS conectadas diretamente • Compartimentos NVMe conectados aos switches IP do MetroCluster É necessário pelo menos um shelf NVMe conectado à Ethernet	9336C-FX2 – armazenamento SAS e Ethernet	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

Antes de começar

Você pode usar esse método se sua configuração atender aos seguintes requisitos:

- A configuração padrão do RCF é aplicada.
- O "RcfFileGenerator" deve ser capaz de criar o mesmo arquivo RCF que é aplicado, com a mesma versão e configuração (plataformas, VLANs).
- O arquivo RCF que é aplicado não foi fornecido pelo NetApp para uma configuração especial.
- O arquivo RCF não foi alterado antes de ser aplicado.
- As etapas para redefinir o switch para os padrões de fábrica foram seguidas antes de aplicar o arquivo RCF atual.
- Não foram feitas alterações na configuração do switch(port) após a aplicação do RCF.

  Se você não atender a esses requisitos, não poderá usar os CleanUpFiles criados ao gerar os arquivos

RCF. No entanto, você pode aproveitar a função para criar CleanUpFiles genéricos — a limpeza usando este método é derivada da saída de `show running-config` e é a melhor prática.

> Você deve atualizar os switches pela seguinte ordem: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. Ou, você pode atualizar os switches Switch_A_1 e Switch_B_1 ao mesmo tempo, seguido pelos switches Switch_A_2 e Switch_B_2.

Passos

1. Determine a versão atual do arquivo RCF e quais portas e VLANs são usadas: `IP_switch_A_1# show banner motd`

> Você precisa obter essas informações de todos os quatro switches e preencher a seguinte tabela de informações.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*


#
IP_switch_A_1#
```

A partir desta saída, você deve coletar as informações mostradas nas duas tabelas a seguir.

Informações genéricas	MetroCluster	Dados
Versão do ficheiro RCF		1,81
Tipo de interrutor		NX9336
Tipologia da rede		L2 redes, ISL direto
Tipo de armazenamento		Storage SAS
Plataformas	1	AFF A400
	2	FAS9000

Informações de VLAN	**Rede**	**Configuração do MetroCluster**	**Portas de comutação**	**Local A**	**Local B**
Cluster local VLAN	Rede 1	1	1, 2	111	222
		2	3, 4	151	251
	Rede 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN MetroCluster	Rede 1	1	9, 10	119	119
		2	11, 12	159	159
	Rede 2	1	9, 10	219	219
		2	11, 12	259	259

2. Crie os arquivos RCF e CleanUpFiles, ou crie CleanUpFiles genéricos para a configuração atual.

   Se sua configuração atender aos requisitos descritos nos pré-requisitos, selecione **opção 1**. Se a sua configuração **não** atender aos requisitos descritos nos pré-requisitos, selecione **opção 2**.

Opção 1: Crie os arquivos RCF e CleanUpFiles

Use este procedimento se a configuração atender aos requisitos.

Passos

a. Use o RcfFileGenerator 1,4a (ou posterior) para criar os arquivos RCF com as informações que você recuperou na Etapa 1. A nova versão do RcfFileGenerator cria um conjunto adicional de CleanUpFiles que você pode usar para reverter alguma configuração e preparar o switch para aplicar uma nova configuração RCF.

b. Compare o banner motd com os arquivos RCF que estão atualmente aplicados. Os tipos de plataforma, tipo de switch, porta e uso de VLAN devem ser os mesmos.

> Você deve usar o CleanUpFiles da mesma versão do arquivo RCF e para a mesma configuração exata. Usar qualquer CleanUpFile não funcionará e pode exigir uma redefinição completa do switch.

> A versão ONTAP para a qual o arquivo RCF foi criado não é relevante. Apenas a versão do arquivo RCF é importante.

> O arquivo RCF (mesmo que seja a mesma versão) pode listar menos ou mais plataformas. Certifique-se de que sua plataforma esteja listada.

Opção 2: Criar CleanUpFiles genéricos

Use este procedimento se a configuração **não** atender a todos os requisitos.

Passos

a. Recupere a saída de de `show running-config` cada interrutor.

b. Abra a ferramenta RcfFileGenerator e clique em 'Create Generic CleanUpFiles' na parte inferior da janela

c. Copie a saída que você recuperou no passo 1 do switch 'one' para a janela superior. Você pode remover ou deixar a saída padrão.

d. Clique em 'criar ficheiros CUF'.

e. Copie a saída da janela inferior para um arquivo de texto (este arquivo é o CleanUpFile).

f. Repita os passos c, d e e para todos os interrutores na configuração.

No final deste procedimento, você deve ter quatro arquivos de texto, um para cada switch. Você pode usar esses arquivos da mesma maneira que os CleanUpFiles que você pode criar usando a opção 1.

3. Crie os arquivos RCF 'new' para a nova configuração. Crie esses arquivos da mesma maneira que você criou os arquivos na etapa anterior, exceto escolha a respetiva versão do arquivo ONTAP e RCF.

   Depois de concluir esta etapa, você deve ter dois conjuntos de arquivos RCF, cada conjunto composto por doze arquivos.

4. Baixe os arquivos para o bootflash.

a. Baixe os CleanUpFiles que você criou Crie os arquivos RCF e CleanUpFiles, ou crie CleanUpFiles genéricos para a configuração atual

> Este CleanUpFile é para o arquivo RCF atual que é aplicado e **NÃO** para o novo RCF para o qual você deseja atualizar.

Exemplo de CleanUpFile para Switch-A1: `Cleanup_NX9336_v1.81_Switch-A1.txt`

b. Transfira os ficheiros RCF "novos" que criou Crie os arquivos RCF 'novos' para a nova configuração.

Exemplo de arquivo RCF para Switch-A1: `NX9336_v1.90_Switch-A1.txt`

c. Baixar o CleanUpFiles que você criou Crie os arquivos RCF 'novos' para a nova configuração.nesta etapa é opcional — você pode usar o arquivo no futuro para atualizar a configuração do switch. Corresponde à configuração atualmente aplicada.

Exemplo de CleanUpFile para Switch-A1: `Cleanup_NX9336_v1.90_Switch-A1.txt`

> Você deve usar o CleanUpFile para a versão RCF correta (correspondente). Se você usar um CleanUpFile para uma versão RCF diferente, ou uma configuração diferente, a limpeza da configuração pode não funcionar corretamente.

O exemplo a seguir copia os três arquivos para o flash de inicialização:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

> É-lhe pedido que especifique o Encaminhamento e Encaminhamento virtuais (VRF).

5. Aplique o CleanUpFile ou o CleanUpFile genérico.

Algumas das configurações são revertidas e switchports ficam "offline".

a. Confirme se não há alterações pendentes na configuração de inicialização: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Se você vir a saída do sistema, salve a configuração em execução na configuração de inicialização: `copy running-config startup-config`

   A saída do sistema indica que a configuração de inicialização e a configuração em execução são alterações diferentes e pendentes. Se você não salvar as alterações pendentes, não será possível reverter usando um recarregamento do switch.

   a. Aplique o CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

   O script pode demorar um pouco para retornar ao prompt do switch. Nenhuma saída é esperada.

7. Exiba a configuração em execução para verificar se a configuração foi limpa: `show running-config`

   A configuração atual deve mostrar:

   - Não estão configurados mapas de classe e listas de acesso IP
   - Nenhum mapa de política está configurado
   - Nenhuma política de serviço está configurada
   - Nenhum perfil de porta está configurado
   - Todas as interfaces Ethernet (exceto mgmt0 que não deve mostrar nenhuma configuração, e somente VLAN 1 deve ser configurada).

     Se você achar que algum dos itens acima está configurado, talvez não seja possível aplicar uma nova configuração de arquivo RCF. No entanto, você pode reverter para a configuração anterior recarregando o switch **sem** salvar a configuração em execução na configuração de inicialização. O interrutor virá com a configuração anterior.

8. Aplique o arquivo RCF e verifique se as portas estão online.

   a. Aplique os arquivos RCF.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

Algumas mensagens de aviso aparecem durante a aplicação da configuração. As mensagens de erro geralmente não são esperadas. No entanto, se você estiver logado usando SSH, poderá receber o seguinte erro: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. Depois que a configuração for aplicada, verifique se o cluster e as portas MetroCluster estão on-line com um dos seguintes comandos, `show interface brief show cdp neighbors` , ou `show lldp neighbors`

Se você alterou a VLAN para o cluster local e atualizou o primeiro switch no local, o monitoramento de integridade do cluster pode não relatar o estado como 'saudável' porque as VLANs das configurações antigas e novas não correspondem. Após a atualização do segundo interrutor, o estado deve retornar à integridade.

Se a configuração não for aplicada corretamente, ou se você não quiser manter a configuração, você pode reverter para a configuração anterior recarregando o switch **sem** salvar a configuração em execução na configuração de inicialização. O interrutor virá com a configuração anterior.

9. Salve a configuração e recarregue o switch.

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Renomeando um switch IP Cisco

Talvez seja necessário renomear um switch IP Cisco para fornecer nomes consistentes em toda a configuração.

Sobre esta tarefa

- Nos exemplos desta tarefa, o nome do switch é alterado de `myswitch` para `IP_switch_A_1`.
- "Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Entre no modo de configuração global:

   `configure terminal`

   O exemplo a seguir mostra o prompt do modo de configuração. Ambos os prompts mostram o nome do switch `myswitch` de .

```
myswitch# configure terminal
myswitch(config)#
```

2. Mudar o nome do switch:

   `switchname new-switch-name`

Se você estiver renomeando ambos os switches na malha, use o mesmo comando em cada switch.

O prompt da CLI muda para refletir o novo nome:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Sair do modo de configuração:

   exit

   O prompt do interrutor de nível superior é exibido:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Copie a configuração atual em execução para o arquivo de configuração de inicialização:

   copy running-config startup-config

5. Verifique se a alteração do nome do switch está visível no prompt do cluster do ONTAP.

   Observe que o novo nome do switch é exibido e o antigo nome do switch (`myswitch`) não aparece.

   a. Entre no modo de privilégio avançado, pressionando **y** quando solicitado
      set -privilege advanced
   b. Exibir os dispositivos conetados
      network device-discovery show
   c. Voltar ao modo de privilégio de administrador
      set -privilege admin

      O exemplo a seguir mostra que o switch aparece com o novo nome `IP_switch_A_1`:

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Adicione, remova ou altere portas ISL sem interrupções nos switches IP Cisco

Talvez seja necessário adicionar, remover ou alterar portas ISL em switches IP Cisco. Você pode converter portas ISL dedicadas para portas ISL compartilhadas ou alterar a

velocidade das portas ISL em um switch IP Cisco.

Sobre esta tarefa

Se você estiver convertendo portas ISL dedicadas para portas ISL compartilhadas, certifique-se de que as novas portas atendam ao "Requisitos para portas ISL compartilhadas".

Você deve concluir todos os passos em ambos os switches para garantir a conetividade ISL.

O procedimento a seguir pressupõe que você esteja substituindo um ISL de 10 GB conetado na porta do switch eth1/24/1 por dois ISLs de 100 GB conetados às portas do switch 17 e 18.

> Se você estiver usando um switch Cisco 9336C-FX2 em uma configuração compartilhada conetando NS224 gavetas, a alteração dos ISLs pode exigir um novo arquivo RCF. Você não precisa de um novo arquivo RCF se sua velocidade atual e nova ISL for 40Gbps e 100Gbps. Todas as outras alterações à velocidade ISL requerem um novo ficheiro RCF. Por exemplo, alterar a velocidade ISL de 40Gbps para 100Gbps não requer um novo arquivo RCF, mas alterar a velocidade ISL de 10Gbps para 40Gbps requer um novo arquivo RCF.

Antes de começar

Consulte a seção **switches** do "NetApp Hardware Universe" para verificar os transcetores suportados.

"Ativar o registo da consola" antes de executar esta tarefa.

Passos

1. Desative as portas ISL dos ISLs em ambos os switches na malha que você deseja alterar.

   > Só é necessário desativar as portas ISL atuais se as estiver a deslocar para uma porta diferente ou se a velocidade do ISL estiver a mudar. Se estiver a adicionar uma porta ISL com a mesma velocidade que as ISLs existentes, avance para o passo 3.

   Você deve inserir apenas um comando de configuração para cada linha e pressionar Ctrl-Z depois de inserir todos os comandos, como mostrado no exemplo a seguir:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/24/1
   switch_A_1(config-if)# shut
   switch_A_1(config-if)#
   switch_A_1#

   switch_B_1# conf t
   switch_B_1(config)# int eth1/24/1
   switch_B_1(config-if)# shut
   switch_B_1(config-if)#
   switch_B_1#
   ```

2. Remova os cabos e transcetores existentes.
3. Altere a porta ISL conforme necessário.

Se você estiver usando switches Cisco 9336C-FX2 em uma configuração compartilhada conetando NS224 gavetas e precisar atualizar o arquivo RCF e aplicar a nova configuração para as novas portas ISL, siga as etapas a. "Atualize os arquivos RCF em switches IP MetroCluster."

Opção	Passo
Para alterar a velocidade de uma porta ISL…	Ligue os novos ISLs às portas designadas de acordo com as respetivas velocidades. Você deve garantir que essas portas ISL para seu switch estejam listadas em *Instalação e Configuração IP do MetroCluster*.
Para adicionar um ISL…	Insira QFSPs nas portas que você está adicionando como portas ISL. Certifique-se de que eles estão listados na *Instalação e Configuração IP do MetroCluster* e faça o cabeamento adequado.

4. Ative todas as portas ISL (se não estiver ativado) em ambos os switches na estrutura começando com o seguinte comando:

   ```
   switch_A_1# conf t
   ```

   Você deve inserir apenas um comando de configuração por linha e pressionar Ctrl-Z depois de inserir todos os comandos:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/17
   switch_A_1(config-if)# no shut
   switch_A_1(config-if)# int eth1/18
   switch_A_1(config-if)# no shut
   switch_A_1(config-if)#
   switch_A_1#
   switch_A_1# copy running-config startup-config

   switch_B_1# conf t
   switch_B_1(config)# int eth1/17
   switch_B_1(config-if)# no shut
   switch_B_1(config-if)# int eth1/18
   switch_B_1(config-if)# no shut
   switch_B_1(config-if)#
   switch_B_1#
   switch_B_1# copy running-config startup-config
   ```

5. Verifique se os ISLs e os canais de porta para os ISLs estão estabelecidos entre ambos os switches:

   ```
   switch_A_1# show int brief
   ```

   Você deve ver as interfaces ISL na saída do comando como mostrado no exemplo a seguir:

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. Repita o procedimento para o tecido 2.

Identificação do armazenamento em uma configuração IP do MetroCluster

Se você precisar substituir um módulo de unidade ou compartimento, primeiro será necessário identificar o local.

Identificação de prateleiras locais e remotas

Quando você visualiza as informações do compartimento de um site do MetroCluster, todas as unidades remotas estão no 0m, o adaptador de host iSCSI virtual. Isto significa que as unidades são acedidas através das interfaces IP MetroCluster. Todas as outras unidades são locais.

Depois de identificar se um compartimento é remoto (no 0m), é possível identificar ainda mais a unidade ou compartimento pelo número de série ou, dependendo das atribuições de ID do compartimento em sua configuração, por ID do compartimento.

Nas configurações IP do MetroCluster que executam o ONTAP 9.4, o ID do compartimento não precisa ser exclusivo entre os sites do MetroCluster. Isso inclui gavetas internas (0) e externas. O número de série é consistente quando visualizado de qualquer nó em qualquer local do MetroCluster.

As IDs de gaveta devem ser exclusivas no grupo de recuperação de desastres (DR), exceto no compartimento interno.

Com o módulo de unidade ou prateleira identificado, você pode substituir o componente usando o procedimento apropriado.

"Mantenha as gavetas de disco DS460C DS224C e DS212C"

Exemplo de saída sysconfig -a

O exemplo a seguir usa o `sysconfig -a` comando para mostrar os dispositivos em um nó na configuração IP do MetroCluster. Esse nó tem as seguintes gavetas e dispositivos anexados:

- Slot 0: Unidades internas (unidades locais)
- Slot 3: ID do compartimento externo 75 e 76 (unidades locais)
- Slot 0: Adaptador de host iSCSI virtual 0m (unidades remotas)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
```

```
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
.
.
.
```

```
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

Adição de gavetas a um IP MetroCluster usando switches MetroCluster de armazenamento compartilhado

Talvez seja necessário adicionar NS224 gavetas a um MetroCluster usando os switches MetroCluster de armazenamento compartilhado.

A partir do ONTAP 9.10,1, você pode adicionar NS224 prateleiras de um MetroCluster usando os switches de armazenamento / MetroCluster compartilhados. Você pode adicionar mais de uma prateleira de cada vez.

Antes de começar

- Os nós devem estar executando o ONTAP 9.9,1 ou posterior.
- Todas as NS224 gavetas atualmente conetadas devem ser conetadas aos mesmos switches que o MetroCluster (configuração de switch MetroCluster / armazenamento compartilhado).
- Este procedimento não pode ser usado para converter uma configuração com prateleiras NS224 conetadas diretamente ou prateleiras NS224 conetadas a switches Ethernet dedicados para uma configuração usando switches MetroCluster / armazenamento compartilhado.
- "Ativar o registo da consola" antes de executar esta tarefa.

Enviar uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Para impedir a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a atualização está em andamento.

   a. Emita o seguinte comando:

      ```
      system node autosupport invoke -node * -type all -message "Maint=10h Adding
      ```

```
or Removing NS224 shelves"_
```

Este exemplo especifica uma janela de manutenção de 10 horas. Você pode querer permitir tempo adicional, dependendo do seu plano.

Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Repita o comando no cluster de parceiros.

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a transição.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verifique se há alertas de integridade em ambos os clusters:

      ```
      system health alert show
      ```

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      ```
      metrocluster show
      ```

   d. Execute uma verificação MetroCluster:

      ```
      metrocluster check run
      ```

   e. Apresentar os resultados da verificação MetroCluster:

      ```
      metrocluster check show
      ```

   f. Execute o Config Advisor.

      "NetApp Downloads: Config Advisor"

   g. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.
2. Verifique se o cluster está em bom estado:

   ```
   cluster show -vserver Cluster
   ```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

3. Verifique se todas as portas do cluster estão ativas:

   `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show -vserver Cluster`

   Cada LIF de cluster deve exibir True para is Home e ter um Administrador de Status/Oper de up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

   `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Aplicando o novo arquivo RCF aos switches

> Se o switch já estiver configurado corretamente, você poderá pular essas próximas seções e ir diretamente para Configurando a criptografia MACsec em switches Cisco 9336C, se aplicável ou para Ligar a nova prateleira NS224.

- É necessário alterar a configuração do switch para adicionar gavetas.
- Você deve rever os detalhes do cabeamento em "Atribuições de porta da plataforma".
- Você deve usar a ferramenta **RcfFileGenerator** para criar o arquivo RCF para sua configuração. O "RcfFileGenerator"também fornece uma visão geral do cabeamento por porta para cada switch. Certifique-se de escolher o número correto de prateleiras. Existem arquivos adicionais criados juntamente com o arquivo RCF que fornecem um layout de cabeamento detalhado que corresponde às suas opções específicas. Use esta visão geral do cabeamento para verificar o cabeamento ao fazer o cabeamento das novas gavetas.

Atualizando arquivos RCF em switches IP MetroCluster

Se você estiver instalando o novo firmware do switch, você deve instalar o firmware do switch antes de atualizar o arquivo RCF.

Este procedimento interrompe o tráfego no switch onde o arquivo RCF é atualizado. O tráfego será retomado quando o novo arquivo RCF for aplicado.

Passos

1. Verifique a integridade da configuração.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

      metrocluster check run

```
cluster_A::*> metrocluster check run
```

A operação é executada em segundo plano.

b. Após a `metrocluster check run` conclusão da operação, execute `metrocluster check show` para visualizar os resultados.

Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Para verificar o estado da operação de verificação MetroCluster em curso, utilizar o comando **`metrocluster operation history show -job-id 38`**

b. Verifique se não há alertas de saúde **`system health alert show`**

2. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

Repor as predefinições de fábrica do interrutor IP do Cisco

Antes de instalar uma nova versão de software e RCFs, você deve apagar a configuração do switch Cisco e executar a configuração básica.

Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.

1. Repor as predefinições de fábrica do interrutor:

a. Apagar a configuração existente: `write erase`

b. Recarregue o software do switch: `reload`

O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt Cancelar provisionamento automático e continuar com a configuração normal?(sim/não)[n], você deve responder `yes` para continuar.

c. No assistente de configuração, introduza as definições básicas do interrutor:

- Palavra-passe de administrador
- Mudar nome
- Configuração de gerenciamento fora da banda
- Gateway predefinido
- Serviço SSH (RSA) depois de concluir o assistente de configuração, o switch reinicializa.

d. Quando solicitado, introduza o nome de utilizador e a palavra-passe para iniciar sessão no comutador.

O exemplo a seguir mostra os prompts e as respostas do sistema ao configurar o switch. Os colchetes de ângulo (<<<) mostram onde você insere as informações.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

Você insere informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e seleciona SSH com RSA.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
   Number of rsa key bits <1024-2048> [1024]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

O conjunto final de prompts completa a configuração:

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Guardar a configuração:

```
IP_switch-A-1# copy running-config startup-config
```

3. Reinicie o switch e aguarde até que o switch recarregue:

```
IP_switch-A-1# reload
```

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Transferir e instalar o software Cisco switch NX-os

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

1. Transfira o ficheiro de software NX-os suportado.

   "Transferência do software Cisco"

2. Copie o software do interrutor para o interrutor: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   Neste exemplo, o arquivo nxos.7.0.3.I4.6.bin é copiado do servidor SFTP 10.10.99.99 para o flash de inicialização local:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verifique em cada switch se os arquivos NX-os estão presentes no diretório bootflash de cada switch: `dir bootflash:`

   O exemplo a seguir mostra que os arquivos estão presentes no IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Instale o software do interrutor: `install all nxos bootflash:nxos.version-number.bin`

   O interrutor recarregará (reiniciará) automaticamente após a instalação do software do interrutor.

   O exemplo a seguir mostra a instalação do software em IP_switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
-- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   Depois que o switch reiniciar, o prompt de login é exibido:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verifique se o software do switch foi instalado: `show version`

   O exemplo a seguir mostra a saída:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Configurando a criptografia MACsec em switches Cisco 9336C

Se desejar, você pode configurar a criptografia MACsec nas portas ISL da WAN que são executadas entre os sites. Você deve configurar o MACsec depois de aplicar o arquivo RCF correto.

A criptografia MACsec só pode ser aplicada às portas ISL WAN.

Requisitos de licenciamento para MACsec

MACsec requer uma licença de segurança. Para obter uma explicação completa do esquema de licenciamento do Cisco NX-os e como obter e solicitar licenças, consulte a. "Guia de licenciamento do Cisco NX-os"

Habilitando ISLs de WAN de criptografia MACsec Cisco em configurações IP MetroCluster

Você pode ativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

1. Entre no modo de configuração global: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Ativar MACsec e MKA no dispositivo: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copie a configuração em execução para a configuração de inicialização: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Desativar encriptação Cisco MACsec

Talvez seja necessário desativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Se desativar a encriptação, também tem de eliminar as suas chaves.

1. Entre no modo de configuração global: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Desative a configuração MACsec no dispositivo: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Selecionar a opção no restaura o recurso MACsec.

3. Selecione a interface que você já configurou com o MACsec.

   Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Remova o chaveiro, a política e o fallback-keychain configurados na interface para remover a configuração do MACsec: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
   keychain fb_kc2
   ```

5. Repita as etapas 3 e 4 em todas as interfaces onde o MACsec está configurado.
6. Copie a configuração em execução para a configuração de inicialização: `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Configurando uma cadeia de chaves e chaves MACsec

Para obter detalhes sobre como configurar uma cadeia de chaves MACsec, consulte a documentação do Cisco para o seu switch.

Ligar a nova prateleira NS224

Passos

1. Instale o kit de montagem em trilho fornecido com a prateleira usando o folheto de instalação fornecido na caixa do kit.
2. Instale e fixe a prateleira nos suportes de suporte e no rack ou gabinete usando o folheto de instalação.
3. Conete os cabos de alimentação à gaveta, prenda-os com o retentor do cabo de alimentação e conete os cabos de alimentação a diferentes fontes de alimentação para obter resiliência.

   Uma prateleira liga-se quando ligada a uma fonte de alimentação; não tem interrutores de alimentação. Quando estiver a funcionar corretamente, o LED bicolor de uma fonte de alimentação acende-se a verde.

4. Defina o ID do compartimento para um número exclusivo no par de HA e na configuração.
5. Conete as portas do compartimento na seguinte ordem:
   a. Ligue o NSM-A, e0a ao interrutor (interrutor-A1 ou interrutor-B1)
   b. Ligue o NSM-B, e0a ao interrutor (interrutor-A2 ou interrutor-B2)
   c. Ligue o NSM-A, e0b ao interrutor (interrutor-A1 ou interrutor-B1)
   d. Ligue o NSM-B, e0b ao interrutor (interrutor-A2 ou interrutor-B2)

6. Use o layout de cabeamento gerado a partir da ferramenta **RcfFileGenerator** para fazer o cabeamento da prateleira às portas apropriadas.

   Depois que o novo compartimento for cabeado corretamente, o ONTAP o detetará automaticamente na rede.

Configurar criptografia de ponta a ponta em uma configuração IP do MetroCluster

A partir do ONTAP 9.15,1, é possível configurar a criptografia de ponta a ponta para criptografar o tráfego de back-end, como NVlog e dados de replicação de armazenamento, entre os sites em uma configuração IP do MetroCluster.

Sobre esta tarefa

- Você deve ser um administrador de cluster para executar esta tarefa.
- Antes de poder configurar a encriptação de ponta a ponta, tem "Configurar o gerenciamento de chaves externas"de .
- Revise os sistemas suportados e a versão mínima do ONTAP necessária para configurar a criptografia de ponta a ponta em uma configuração IP do MetroCluster:

Versão mínima de ONTAP	Sistemas suportados
ONTAP 9.15,1	• AFF A400 • FAS8300 • FAS8700

Ative a criptografia de ponta a ponta

Execute as etapas a seguir para habilitar a criptografia de ponta a ponta.

Passos

1. Verifique a integridade da configuração do MetroCluster.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   A operação é executada em segundo plano.

   b. Após `metrocluster check run` a conclusão da operação, execute:

   ```
   metrocluster check show
   ```

Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id <id>
```

b. Verifique se não há alertas de saúde:

```
system health alert show
```

2. Verifique se o gerenciamento de chaves externas está configurado em ambos os clusters:

```
security key-manager external show-status
```

3. Habilite a criptografia de ponta a ponta para cada grupo de DR:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Exemplo

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Repita esta etapa para cada grupo de DR na configuração.

4. Verifique se a criptografia de ponta a ponta está ativada:

```
metrocluster node show -fields is-encryption-enabled
```

Exemplo

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

Desative a criptografia de ponta a ponta

Execute as etapas a seguir para desativar a criptografia de ponta a ponta.

Passos

1. Verifique a integridade da configuração do MetroCluster.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   A operação é executada em segundo plano.

b. Após `metrocluster check run` a conclusão da operação, execute:

```
metrocluster check show
```

Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id <id>
```

b. Verifique se não há alertas de saúde:

```
system health alert show
```

2. Verifique se o gerenciamento de chaves externas está configurado em ambos os clusters:

```
security key-manager external show-status
```

3. Desative a criptografia de ponta a ponta em cada grupo de DR:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Exemplo

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Repita esta etapa para cada grupo de DR na configuração.

4. Verifique se a criptografia de ponta a ponta está desativada:

```
metrocluster node show -fields is-encryption-enabled
```

Exemplo

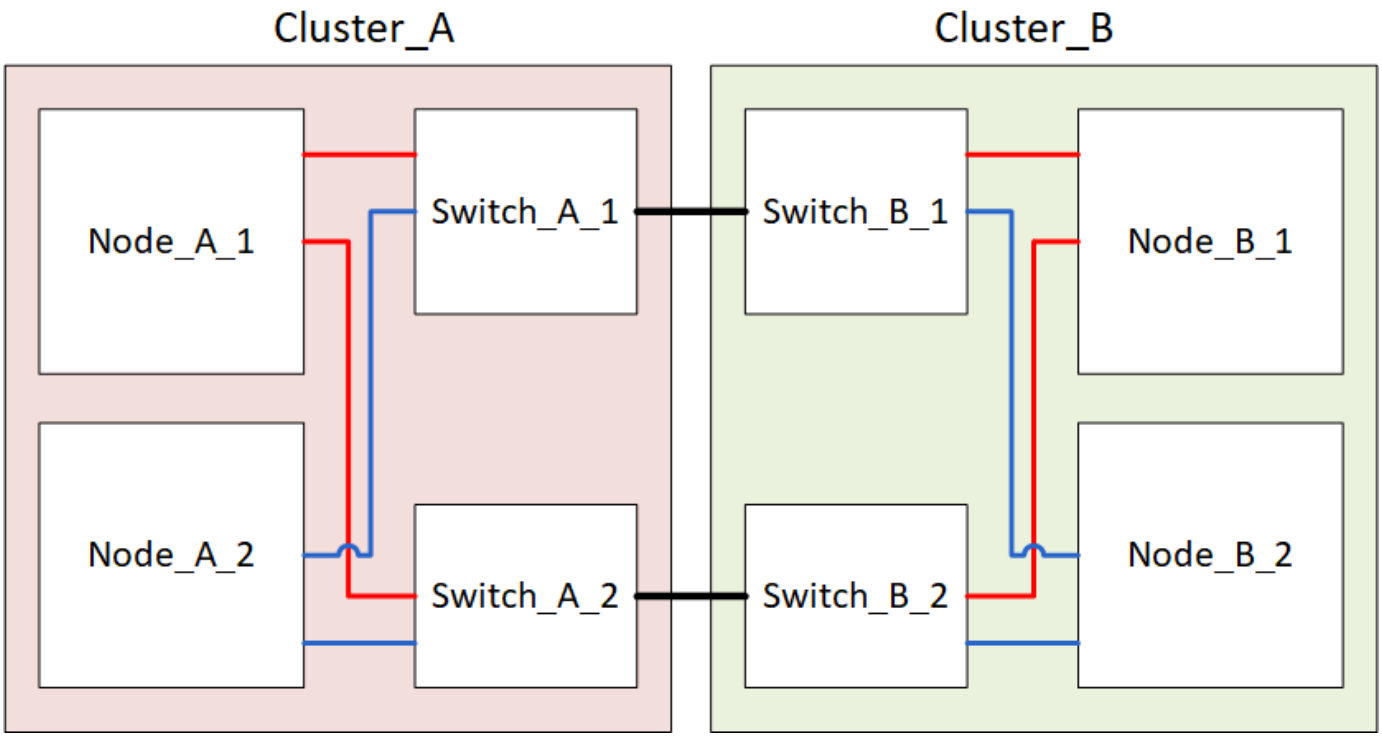
```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Desligue e ligue um único local numa configuração IP MetroCluster

Se você precisar executar a manutenção do local ou realocar um único local em uma configuração IP do MetroCluster, você deve saber como desligar e ligar o local.

Se você precisar realocar e reconfigurar um local (por exemplo, se precisar expandir de um cluster de quatro nós para um cluster de oito nós), não será possível concluir essas tarefas ao mesmo tempo. Este procedimento abrange apenas as etapas necessárias para realizar a manutenção do local ou para realocar um local sem alterar sua configuração.

O diagrama a seguir mostra uma configuração do MetroCluster. Cluster_B está desligado para manutenção.



Desligue um site da MetroCluster

Você deve desligar um local e todo o equipamento antes que a manutenção ou realocação do local possa começar.

Sobre esta tarefa

Todos os comandos nas etapas a seguir são emitidos a partir do site que permanece ligado.

Passos

1. Antes de começar, verifique se todos os agregados não espelhados no site estão offline.
2. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      `node run -node node-name sysconfig -a`

   b. Verifique se há alertas de integridade em ambos os clusters:

      `system health alert show`

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

   d. Execute uma verificação MetroCluster
      `metrocluster check run`
   e. Apresentar os resultados da verificação MetroCluster:

      `metrocluster check show`

f. Verifique se existem alertas de estado nos interrutores (se presentes):

```
storage switch show
```

g. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

3. A partir do local em que você deseja permanecer ativo, implemente o switchover:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

A operação pode levar vários minutos para ser concluída.

4. Monitorize e verifique a conclusão do switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Se você tiver uma configuração IP do MetroCluster executando o ONTAP 9.6 ou posterior, aguarde que os plexes do local de desastre fiquem online e as operações de recuperação sejam concluídas automaticamente.

Nas configurações IP do MetroCluster executando o ONTAP 9.5 ou anterior, os nós do local de desastre não são inicializados automaticamente no ONTAP e os plexos permanecem offline.

6. Mova todos os volumes e LUNs que pertençam a agregados sem espelhamento offline.

a. Mova os volumes offline.

```
cluster_A::* volume offline <volume name>
```

b. Mova os LUNs off-line.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Mover agregados sem espelhamento offline: `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. Dependendo da configuração e da versão do ONTAP, identifique e mova os plexos afetados offline que estão localizados no local de desastre (Cluster_B).

   Você deve mover os seguintes plexes off-line:

   - Plexos não espelhados residentes em discos localizados no local de desastre.

     Se você não mover os plexos não espelhados no local de desastre off-line, uma interrupção pode ocorrer quando o local de desastre for desligado mais tarde.

   - Plexos espelhados que residem em discos localizados no local de desastre para espelhamento agregado. Depois que eles são movidos off-line, os plexes são inacessíveis.

   a. Identificar os plexos afetados.

      Os plexes que são propriedade de nós no local sobrevivente consistem em Pool1 discos. Os plexes que são propriedade de nós no local de desastre consistem em Pool0 discos.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

Os plexos afetados são aqueles que são remotos para o cluster A. a tabela a seguir mostra se os discos são locais ou remotos em relação ao cluster A:

Nó	Discos no pool	Os discos devem ser configurados offline?	Exemplo de plexes a serem movidos off-line
Nó _A_1 e nó _A_2	Discos no pool 0	Os discos não são locais para o cluster A..	-
Discos no pool 1	Sim. Os discos são remotos para o cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nó _B_1 e nó _B_2

Discos no pool 0	Sim. Os discos são remotos para o cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Discos no pool 1

b. Mova os plexes afetados offline:

`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

Execute esta etapa para todos os plexos que têm discos remotos para Cluster_A.

9. Persistentemente offline as portas do switch ISL de acordo com o tipo de switch.
10. Interrompa os nós executando o seguinte comando em cada nó:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Desligue o equipamento no local do desastre.

Tem de desligar o seguinte equipamento pela ordem indicada:

- Controladores de armazenamento - os controladores de armazenamento devem estar `LOADER` no prompt, você deve desligá-los completamente.
- Switches IP MetroCluster
- Prateleiras de storage

Mudar o local desligado do MetroCluster

Depois de o site ser desligado, você pode começar o trabalho de manutenção. O procedimento é o mesmo se os componentes do MetroCluster forem relocados no mesmo data center ou relocados para um data center diferente.

- O hardware deve ser cabeado da mesma forma que o site anterior.
- Se a velocidade, o comprimento ou o número do enlace inter-switch (ISL) tiverem sido alterados, todos eles precisam ser reconfigurados.

Passos

1. Verifique se o cabeamento de todos os componentes é cuidadosamente gravado para que ele possa ser reconetado corretamente no novo local.
2. Realocar fisicamente todo o hardware, controladores de armazenamento, switches IP, FibreBridges e compartimentos de armazenamento.
3. Configure as portas ISL e verifique a conetividade entre sites.

a. Ligue os interrutores IP.

Não ligue nenhum outro equipamento.

4. Use ferramentas nos switches (conforme disponíveis) para verificar a conetividade entre sites.

Você só deve prosseguir se os links estiverem corretamente configurados e estáveis.

5. Desative os links novamente se eles forem encontrados estáveis.

Ligar a configuração do MetroCluster e regressar ao funcionamento normal

Após a manutenção ter sido concluída ou o site ter sido movido, você deve ligar o site e restabelecer a configuração do MetroCluster.

Sobre esta tarefa

Todos os comandos nas etapas a seguir são emitidos a partir do site em que você liga.

Passos

1. Ligue os interrutores.

   Deve ligar primeiro os interrutores. Eles podem ter sido ligados durante a etapa anterior se o local foi transferido.

   a. Reconfigure a ligação entre interrutores (ISL), se necessário, ou se esta não tiver sido concluída como parte da realocação.

   b. Ative o ISL se a vedação tiver sido concluída.

   c. Verifique o ISL.

2. Ligue os controladores de armazenamento e aguarde até que você veja o `LOADER` prompt. Os controladores não devem ser totalmente inicializados.

   Se a inicialização automática estiver ativada, pressione `Ctrl+C` para impedir que os controladores iniciem automaticamente.

3. Ligue as prateleiras, permitindo tempo suficiente para que elas se liguem completamente.

4. Verifique se o armazenamento está visível.

   a. Verifique se o armazenamento está visível a partir do local sobrevivente. Coloque os plexes offline novamente online para reiniciar a operação ressincronizada e restabelecer o SyncMirror.

   b. Verifique se o armazenamento local está visível a partir do nó no modo Manutenção:

   ```
   disk show -v
   ```

5. Restabelecer a configuração do MetroCluster.

   Siga as instruções em "Verificando se o sistema está pronto para um switchback" para executar operações de recuperação e switchback de acordo com sua configuração do MetroCluster.

Desligar toda uma configuração IP do MetroCluster

Você deve desligar toda a configuração IP do MetroCluster e todo o equipamento antes que a manutenção ou realocação possa começar.

> A partir de ONTAP 9.8, o **`storage switch`** comando é substituído por **`system switch`**. As etapas a seguir mostram o **`storage switch`** comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o **`system switch`** comando é preferido.

1. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.
   a. Confirme se a configuração do MetroCluster e o modo operacional estão normais. E
      `metrocluster show`
   b. Execute o seguinte comando
      `metrocluster interconnect show`
   c. Confirme a conetividade com os discos inserindo o seguinte comando em qualquer um dos nós MetroCluster
      `run local sysconfig -v`
   d. Execute o seguinte comando
      `storage port show`
   e. Execute o seguinte comando
      `storage switch show`
   f. Execute o seguinte comando
      `network interface show`
   g. Execute o seguinte comando
      `network port show`
   h. Execute o seguinte comando
      `network device-discovery show`
   i. Execute uma verificação MetroCluster
      `metrocluster check run`
   j. Exibir os resultados da verificação MetroCluster
      `metrocluster check show`
   k. Execute o seguinte comando
      `metrocluster configuration-settings interface show`
2. Se necessário, desative o AUSO modificando o domínio de falha do AUSO para

   `auso-disabled`

   ```
   cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
   auso-disabled
   ```

   > Em uma configuração IP do MetroCluster, o domínio de falha do AUSO já está definido como 'AUSO-Disabled', a menos que a configuração seja configurada com o Mediador do ONTAP.

3. Verifique a alteração usando o comando

   metrocluster operation show

   ```
   cluster_A_site_A::*> metrocluster operation show
      Operation: modify
          State: successful
     Start Time: 4/25/2020 20:20:36
       End Time: 4/25/2020 20:20:36
         Errors: -
   ```

4. Parar os nós:

   halt

   ```
   system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
   -warnings true
   ```

5. Desligue o seguinte equipamento no local:
   - Controladores de storage
   - Switches IP MetroCluster
   - Prateleiras de storage
6. Aguarde trinta minutos e ligue todos os compartimentos de storage, switches IP MetroCluster e controladores de storage.
7. Depois que os controladores estiverem ligados, verifique a configuração do MetroCluster de ambos os sites.

   Para verificar a configuração, repita a etapa 1.

8. Execute as verificações do ciclo de alimentação.
   a. Verifique se todas as SVMs de origem sincronizada estão online
   vserver show
   b. Inicie qualquer SVMs de origem sincronizada que não estejam online
   vserver start

Procedimentos de manutenção para todas as configurações do MetroCluster

Substituição de uma gaveta sem interrupções em uma configuração Stretch MetroCluster

Você pode substituir os compartimentos de disco sem interrupção em uma configuração Stretch MetroCluster por um compartimento de disco totalmente preenchido ou um chassi de compartimento de disco e transferir componentes da gaveta que você está

removendo.

O modelo de compartimento de disco que você está instalando deve atender aos requisitos de sistema de storage especificados no "Hardware Universe", que inclui modelos de gaveta compatíveis, tipos de unidades de disco compatíveis, o número máximo de compartimentos de disco em uma pilha e versões ONTAP compatíveis.

Passos

1. Aterre-se corretamente.
2. Identifique todos os agregados e volumes que têm discos do loop que contém a gaveta que você está substituindo e anote o nome do Plex afetado.

   Qualquer nó pode conter discos do loop da gaveta afetada e agregados de host ou volumes de host.

3. Escolha uma das duas opções a seguir com base no cenário de substituição que você está planejando.
   - Se você estiver substituindo um compartimento de disco completo, incluindo o chassi da gaveta, discos e módulos de e/S (IOM), execute a ação correspondente conforme descrito na tabela abaixo:

Cenário	Ação
O Plex afetado contém menos discos da gaveta afetada.	Substitua os discos um a um na gaveta afetada por peças sobressalentes de outra gaveta. Você pode colocar o Plex off-line depois de concluir a substituição do disco.
O Plex afetado contém mais discos do que na gaveta afetada.	Mova o Plex off-line e, em seguida, exclua o Plex.
O Plex afetado tem qualquer disco da prateleira afetada.	Mova o Plex off-line, mas não o exclua.

   - Se você estiver substituindo apenas o chassi do compartimento de disco e nenhum outro componente, execute as seguintes etapas:
     i. Offline os plexes afetados do controlador onde estão hospedados:

     ```
     aggregate offline
     ```

     ii. Verifique se os plexes estão offline:

     ```
     aggregate status -r
     ```

4. Identifique as portas SAS da controladora às quais o loop do compartimento afetado está conetado e desative as portas SAS em ambos os controladores do local:

   ```
   storage port disable -node node_name -port SAS_port
   ```

   O loop de prateleira afetado é conetado a ambos os locais.

5. Aguarde que o ONTAP reconheça que o disco está ausente.

a. Verifique se o disco está em falta:

`sysconfig -a` ou `sysconfig -r`

6. Desligue o interrutor de alimentação no compartimento de disco.
7. Desconete todos os cabos de energia do compartimento de disco.
8. Faça um Registro das portas a partir das quais você desconete os cabos para que você possa fazer o cabeamento da nova gaveta de disco da mesma maneira.
9. Desconete e remova os cabos que conetam o compartimento de disco às outras gavetas de disco ou ao sistema de storage.
10. Remova o compartimento de disco do rack.

    Para tornar o compartimento de disco mais leve e fácil de manobrar, remova as fontes de alimentação e a IOM. Se você estiver instalando um chassi de compartimento de disco, remova também as unidades de disco ou as operadoras. Caso contrário, evite remover unidades de disco ou transportadores, se possível, porque o manuseio excessivo pode causar danos internos na unidade.

11. Instale e fixe o compartimento de disco de substituição nos suportes de suporte e no rack.
12. Se você instalou um chassi de compartimento de disco, reinstale as fontes de alimentação e IOM.
13. Reconfigure a pilha de compartimentos de disco conetando todos os cabos às portas do compartimento de disco de substituição exatamente como eles foram configurados no compartimento de disco que você removeu.
14. Ligue a alimentação do compartimento de disco de substituição e aguarde até que as unidades de disco girem.
15. Altere a ID do compartimento de disco para uma ID exclusiva de 0 a 98.
16. Ative todas as portas SAS que você desativou anteriormente .
    a. Aguarde que o ONTAP reconheça que os discos estão inseridos.
    b. Verifique se os discos estão inseridos:

    `sysconfig -a` ou `sysconfig -r`

17. Se estiver substituindo a gaveta de disco completa (chassi da gaveta de disco, discos, IOM), execute o seguinte procedimento:

    Se estiver a substituir apenas o chassis do compartimento de disco e nenhum outro componente, avance para o passo 19.

    a. Determine se a atribuição automática de disco está ativada (ligada).

    `storage disk option modify -autoassign`

    A atribuição de disco ocorrerá automaticamente.

    a. Se a atribuição automática do disco não estiver ativada, atribua a propriedade do disco manualmente.
18. Mova os plexes de volta online:

    `aggregate online` *`plex name`*

19. Recrie quaisquer plexes que foram excluídos espelhando o agregado.
20. Monitorize os plexos à medida que começam a ressincronizar:

```
aggregate status -r <aggregate name>
```

21. Verifique se o sistema de armazenamento está funcionando conforme esperado:

```
system health alert show
```

Quando migrar volumes raiz para um novo destino

Talvez seja necessário mover volumes raiz para outro agregado de raiz em uma configuração de MetroCluster de dois nós ou quatro nós.

Migração de volumes raiz em uma configuração de MetroCluster de dois nós

Para migrar volumes de raiz para um novo agregado de raiz em uma configuração de MetroCluster de dois nós, "Como mover o mroot para um novo agregado de raiz em um MetroCluster em cluster de 2 nós com switchover" consulte o . Esse procedimento mostra como migrar os volumes raiz sem interrupções durante uma operação de switchover do MetroCluster. Este procedimento é ligeiramente diferente do procedimento utilizado numa configuração de quatro nós.

Migração de volumes raiz em uma configuração de MetroCluster de quatro nós

Para migrar volumes raiz para um novo agregado raiz em uma configuração de MetroCluster de quatro nós, você pode usar o "raiz de migração do nó do sistema" comando enquanto atende aos requisitos a seguir.

- Você pode usar a migração-raiz de nó do sistema para mover agregados de raiz em uma configuração de MetroCluster de quatro nós.
- Todos os agregados de raiz devem ser espelhados.
- Você pode adicionar novas gavetas em ambos os locais com unidades menores para hospedar o agregado de raiz.
- Você deve verificar os limites de unidade suportados pela plataforma antes de conetar novas unidades.

  "NetApp Hardware Universe"

- Se você mover o agregado raiz para unidades menores, precisará acomodar o tamanho mínimo do volume raiz da plataforma para garantir que todos os arquivos principais sejam salvos.

O procedimento de quatro nós também pode ser aplicado a uma configuração de oito nós.

Movimentação de um volume de metadados nas configurações do MetroCluster

Você pode mover um volume de metadados de um agregado para outro agregado em uma configuração do MetroCluster. Talvez você queira mover um volume de metadados quando o agregado de origem for desativado ou sem espelhamento, ou por outros motivos que tornam o agregado inelegível.

- Você deve ter o administrador de cluster Privileges para executar esta tarefa.

- O agregado de destino deve ser espelhado e não deve estar no estado degradado.
- O espaço disponível no agregado de destino deve ser maior que o volume de metadados que você está movendo.

Passos

1. Defina o nível de privilégio como avançado:

   set -privilege advanced

2. Identifique o volume de metadados que deve ser movido:

   volume show MDV_CRS*

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identificar um agregado-alvo qualificado:

   metrocluster check config-replication show-aggregate-eligibility

   O comando a seguir identifica os agregados em cluster_A que estão qualificados para hospedar volumes

de metadados:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ -------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

No exemplo anterior, Node_A_1_aggr2 e Node_A_2_aggr2 são elegíveis.

4. Iniciar a operação de movimentação de volume:

volume move start -vserver *svm_name* -volume *metadata_volume_name* -destination -aggregate *destination_aggregate_name*

O comando a seguir move o volume de metadados `MDV_CRS_14c00d4ac9f311e7922800a0984395f1` de `aggregate Node_A_1_aggr1` para `aggregate Node_A_1_aggr2`:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verifique o estado da operação de movimentação de volume:

   volume move show -volume vol_constituent_name

6. Voltar ao nível de privilégio de administrador:

   set -privilege admin

Renomeando um cluster nas configurações do MetroCluster

Renomear um cluster em uma configuração do MetroCluster envolve fazer as alterações e, em seguida, verificar nos clusters locais e remotos se a alteração entrou em vigor corretamente.

Passos

1. Visualize os nomes do cluster utilizando o.

   metrocluster node show

   comando:

```
cluster_1::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_1
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

2. Renomeie o cluster:

   cluster identity modify -name *new_name*

   No exemplo a seguir, o `cluster_1` cluster é renomeado `cluster_A`:

```
cluster_1::*> cluster identity modify -name cluster_A
```

3. Verifique no cluster local se o cluster renomeado está sendo executado normalmente:

   metrocluster node show

   No exemplo a seguir, o recém-renomeado `cluster_A` está sendo executado normalmente:

```
cluster_A::*> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1          configured     enabled   normal
              node_A_2          configured     enabled   normal
      cluster_2
              node_B_1          configured     enabled   normal
              node_B_2          configured     enabled   normal
4 entries were displayed.
```

4. Mudar o nome do cluster remoto:

   `cluster peer modify-local-name -name cluster_2 -new-name cluster_B`

   No exemplo a seguir, `cluster_2` é renomeado `cluster_B`:

```
cluster_A::> cluster peer modify-local-name -name cluster_2 -new-name
cluster_B
```

5. Verifique no cluster remoto se o cluster local foi renomeado e está sendo executado normalmente:

   `metrocluster node show`

   No exemplo a seguir, o recém-renomeado `cluster_B` está sendo executado normalmente:

```
cluster_B::*> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_B
              node_B_1          configured     enabled   normal
              node_B_2          configured     enabled   normal
      cluster_A
              node_A_1          configured     enabled   normal
              node_A_2          configured     enabled   normal
4 entries were displayed.
```

6. Repita estas etapas para cada cluster que você deseja renomear.

Verifique a integridade de uma configuração do MetroCluster

Saiba como verificar se os componentes do MetroCluster estão saudáveis.

Sobre esta tarefa

- Nas configurações MetroCluster IP e FC, você pode usar a CLI para executar comandos de verificação de integridade e verificar o estado dos componentes do MetroCluster.
- Nas configurações IP do MetroCluster executando o ONTAP 9.8 ou posterior, você também pode usar o Gerenciador do sistema ONTAP para monitorar e solucionar problemas de alertas de verificação de integridade.

Passos

Verifique a integridade da configuração do MetroCluster dependendo se você está usando a CLI ou o Gerenciador de sistema.

CLI

Siga as etapas a seguir para verificar a integridade de uma configuração do MetroCluster usando a CLI.

Passos

1. Verifique se os componentes do MetroCluster estão em bom estado:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

A operação é executada em segundo plano.

2. Após a `metrocluster check run` conclusão da operação, exiba os resultados:

```
metrocluster check show
```

Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

3. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

```
metrocluster operation history show -job-id <id>
```

4. Verifique se não há alertas de saúde:

```
system health alert show
```

Gerenciador do sistema ONTAP (somente MetroCluster IP)

A partir do ONTAP 9.8, o Gerenciador do sistema monitora a integridade das configurações IP do MetroCluster e ajuda a identificar e corrigir problemas que possam ocorrer.

O Gerenciador do sistema verifica periodicamente a integridade da configuração IP do MetroCluster. Quando você visualiza a seção MetroCluster no Painel de Controle, geralmente a mensagem é "os sistemas MetroCluster estão saudáveis".

No entanto, quando ocorrer um problema, a mensagem mostrará o número de eventos. Você pode clicar nesta mensagem e exibir os resultados da verificação de integridade dos seguintes componentes:

- Nó
- Interface de rede
- Camada (storage)
- Cluster
- Ligação
- Volume
- Replicação de configuração

A coluna **Status** identifica quais componentes têm problemas e a coluna **Detalhes** sugere como corrigir o problema.

Passos

1. No System Manager, selecione **Dashboard**.
2. Veja a mensagem na seção **MetroCluster**:
   a. Se a mensagem indicar que a configuração do MetroCluster está saudável e as conexões entre os clusters e o Mediador do ONTAP estão saudáveis (mostradas com marcas de verificação), então você não terá problemas para corrigir.
   b. Se a mensagem indicar o número de eventos ou se as ligações tiverem diminuído (apresentado com um "X"), avance para o passo seguinte.
3. Clique na mensagem que mostra o número de eventos.

   É apresentado o Relatório de estado do MetroCluster.

4. Solucione os problemas que aparecem no relatório usando as sugestões na coluna **Detalhes**.
5. Quando todos os problemas tiverem sido corrigidos, clique em **verificar o estado do MetroCluster**.

   Você deve executar todas as tarefas de solução de problemas antes de executar a verificação porque a Verificação de integridade do MetroCluster usa uma quantidade intensiva de recursos.

   A Verificação de integridade do MetroCluster é executada em segundo plano. Você pode trabalhar em outras tarefas enquanto espera que ele termine.

Onde encontrar informações adicionais

Você pode saber mais sobre como configurar, operar e monitorar uma configuração do MetroCluster na extensa documentação do NetApp.

Informações	Assunto
"Documentação do MetroCluster"	• Todas as informações do MetroCluster
"Arquitetura e design da solução NetApp MetroCluster"	• Uma visão geral técnica da configuração e operação do MetroCluster. • Práticas recomendadas para a configuração do MetroCluster.
"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Instalação e configuração IP do MetroCluster"	• Arquitetura IP do MetroCluster • Cabeamento da configuração IP do MetroCluster • Configurando o MetroCluster no ONTAP
"Documentação do NetApp: Guias de produto e recursos"	• Monitoramento da configuração e do desempenho do MetroCluster
"Instalação e configuração do software MetroCluster Tiebreaker"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster

Transição do MetroCluster FC para o MetroCluster IP

Escolha o procedimento de transição

Ao fazer a transição para uma configuração IP do MetroCluster, você deve ter uma combinação de modelos de plataforma compatíveis.

Você também deve garantir que a plataforma IP do MetroCluster seja um tamanho apropriado para a carga que você está migrando da configuração do MetroCluster FC para a configuração IP do MetroCluster.

Combinações de plataformas suportadas

- Todos os procedimentos de transição requerem ONTAP 9.8 ou posterior, salvo indicação em contrário nas notas ou conforme exigido por uma plataforma individual.
- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do ONTAP. Por exemplo, se você tiver uma configuração de oito nós, todos os oito nós devem estar executando a mesma versão do ONTAP.

- Não exceda quaisquer limites de objeto do "inferior" das plataformas na combinação. Aplique o limite inferior de objetos das duas plataformas.
- Se os limites da plataforma de destino forem inferiores aos limites do MetroCluster, você deverá reconfigurar o MetroCluster para estar nos limites da plataforma de destino ou inferiores antes de adicionar os novos nós.
- Consulte a "Hardware Universe"para obter os limites da plataforma.

Combinações de transição AFF e FAS suportadas

A tabela a seguir mostra as combinações de plataforma suportadas. Você pode fazer a transição de plataformas na coluna esquerda para plataformas listadas como suportadas nas colunas para a direita, conforme indicado pelas células da tabela coloridas.

Por exemplo, a transição de uma configuração MetroCluster FC que consiste em módulos de controlador AFF8060 para uma configuração IP que consiste em módulos de controlador AFF A400 é suportada.

AFF and FAS		Target MetroCluster IP platform												
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF A90	AFF A1K
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040													
	FAS8060 AFF8060 FAS8080 AFF8080													
	FAS8200 AFF A300			Note 1										
	FAS8300 AFF A400													
	FAS9000 AFF A700								Note 2	Note 2	Note 2	Note 2	Note 2	Note 2
	FAS9500 AFF A900											Note 3	Note 3	Note 3

- Nota 1: Esta combinação de plataforma requer ONTAP 9.11,1 ou posterior.

- Observação 2: Você precisa ter uma interface 40GbE para as interfaces de cluster local nos nós FC.
- Observação 3: Você precisa ter uma interface 100GbE para as interfaces de cluster local nos nós FC.

Combinações de plataforma de transição ASA suportadas

A tabela a seguir mostra as combinações de plataforma suportadas para sistemas ASA.

Fonte da plataforma MetroCluster FC	Plataforma IP MetroCluster de destino	Suportado?
ASA A400	ASA A400	Sim
	ASA A900	Não
ASA A900	ASA A400	Não
	ASA A900	Sim

Escolha o procedimento de transição

Você deve selecionar um procedimento de transição dependendo da configuração existente do MetroCluster FC.

Um procedimento de transição substitui a malha de switch FC de back-end ou a conexão FC-VI por uma rede de switch IP. O procedimento exato depende da configuração inicial.

As plataformas originais e os switches FC (se presentes) são desativados no final do procedimento de transição.

A iniciar a configuração	Interrupções ou interrupções	Requisitos	Procedimento
Quatro ou oito nós	Sem interrupções	Novas gavetas de storage são compatíveis com novas plataformas.	"Ligação ao procedimento"
Dois nós	Interrupções	Novas gavetas de storage são compatíveis com plataformas originais e novas.	"Ligação ao procedimento"
Dois nós	Interrupções	Novas gavetas de storage são compatíveis com plataformas originais e novas. É preciso desativar as gavetas de storage antigas.	"Ligação ao procedimento"

Dois nós	Interrupções	Compartimentos de storage antigos não são compatíveis com novas plataformas. É preciso desativar as gavetas de storage antigas.	"Ligação ao procedimento"

Transição sem interrupções de um MetroCluster FC para uma configuração MetroCluster IP (ONTAP 9.8 e posterior)

Transição de uma configuração IP do MetroCluster FC para uma configuração IP do MetroCluster sem interrupções (ONTAP 9.8 e posterior)

Você pode fazer transições sem interrupções de workloads e dados de uma configuração MetroCluster FC existente para uma nova configuração MetroCluster IP.

A partir do ONTAP 9.13,1, esse procedimento é compatível com configurações IP do MetroCluster nas quais o MetroCluster e os compartimentos de unidades são conetados aos mesmos switches IP (uma configuração de switch de armazenamento compartilhado).

A partir do ONTAP 9.13,1, você faz uma transição sem interrupções de workloads e dados de uma configuração MetroCluster FC de oito nós existente para uma nova configuração MetroCluster IP.

A partir do ONTAP 9.8, você faz uma transição sem interrupções de workloads e dados de uma configuração MetroCluster FC de quatro nós existente para uma nova configuração MetroCluster IP.

- Esse procedimento não causa interrupções.

  A configuração do MetroCluster pode continuar fornecendo dados durante a operação.

- Esse procedimento se aplica apenas a configurações de FC MetroCluster de quatro nós e oito nós.

  Se você tiver uma configuração MetroCluster FC de dois nós, "Escolhendo seu procedimento de transição"consulte .

- Este procedimento descreve as etapas necessárias para fazer a transição de um grupo de RD FC de quatro nós. Se você tiver uma configuração de oito nós (dois grupos de DR FC), repita todo o procedimento para cada grupo de DR FC.
- Você deve atender a todos os requisitos e seguir todas as etapas do procedimento.

Prepare-se para a transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP

Ativar o registo da consola

Ative o registo da consola nos seus dispositivos antes de executar esta tarefa.

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e

execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Requisitos para transição FC para IP sem interrupções

Antes de iniciar o processo de transição, você deve garantir que a configuração atenda aos requisitos.

- Se você tiver uma configuração de oito nós, todos os nós devem estar executando o ONTAP 9.13,1 ou posterior.
- Se você tiver uma configuração de quatro nós, todos os nós devem estar executando o ONTAP 9.8 ou posterior.
- As plataformas existentes e novas devem ser uma combinação suportada para a transição.

  "Plataformas compatíveis para transição sem interrupções"

- Ele deve suportar uma configuração de cluster comutada.

  "NetApp Hardware Universe"

- Ele deve atender a todos os requisitos e cabeamento, conforme descrito nos procedimentos *Instalação e Configuração do MetroCluster*.

  "Instalação e configuração do MetroCluster conectado à malha"

  "Instalação e configuração do Stretch MetroCluster"

Como a transição afeta os componentes de hardware do MetroCluster

Após concluir o procedimento de transição, os componentes principais da configuração do MetroCluster existente foram substituídos ou reconfigurados.

- **Módulos de controlador**

  Os módulos do controlador existentes são substituídos por novos módulos do controlador. Os módulos de controlador existentes são desativados no final dos procedimentos de transição.

- * Prateleiras de armazenamento*

  Os dados são movidos das gavetas antigas para as novas gavetas. As prateleiras antigas são desativadas no final dos procedimentos de transição.

- **MetroCluster (back-end) e switches de cluster**

  A funcionalidade do switch back-end é substituída pela malha do switch IP. Se a configuração de FC do MetroCluster incluir switches FC e pontes FC para SAS, eles serão desativados no final deste procedimento.

  Se a configuração MetroCluster FC usou switches de cluster para a interconexão de cluster, em alguns casos eles podem ser reutilizados para fornecer a malha de switch IP de back-end. Os switches de cluster reutilizados devem ser reconfigurados com os procedimentos de CFs específicos da plataforma e do switch.

  Se a configuração MetroCluster FC não usasse switches de cluster, novos switches IP serão adicionados para fornecer a malha do switch de back-end.

  "Considerações para switches IP"

- **Rede de peering de cluster**

  A rede de peering de cluster existente fornecida pelo cliente pode ser usada para a nova configuração IP do MetroCluster. O peering de cluster é configurado nos nós IP do MetroCluster como parte do procedimento de transição.

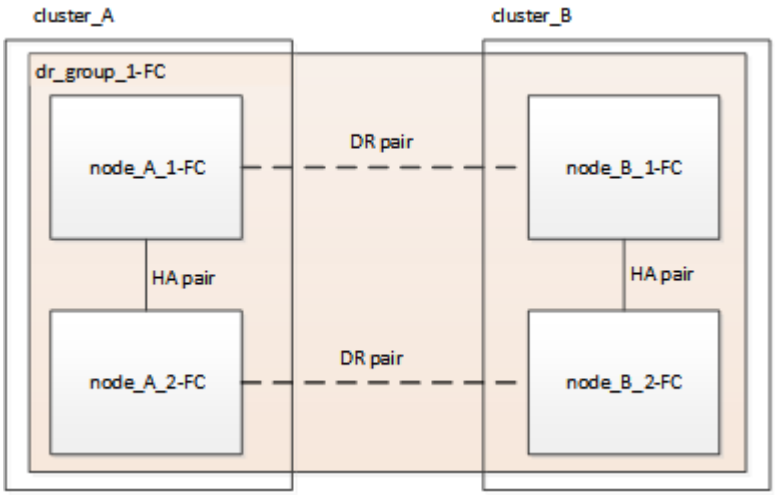
Fluxo de trabalho para transição sem interrupções de MetroCluster

Siga o fluxo de trabalho específico para garantir uma transição sem interrupções bem-sucedida. Escolha o fluxo de trabalho para sua configuração:

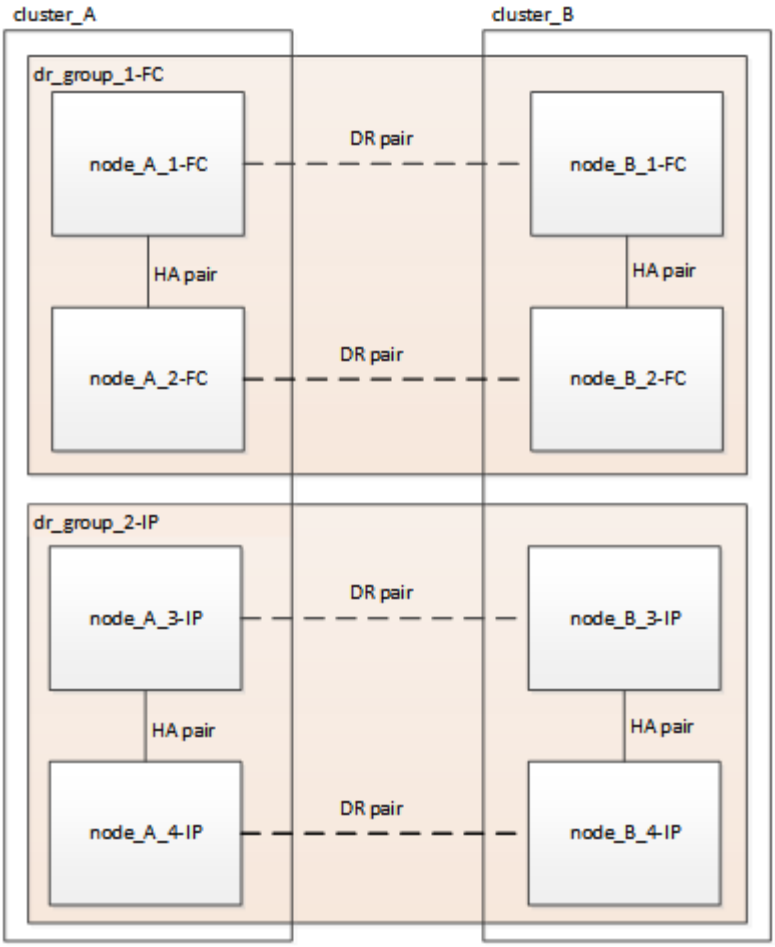
- Fluxo de trabalho de transição de configuração de FC de quatro nós
- Fluxo de trabalho de transição de configuração de FC de oito nós

Fluxo de trabalho de transição de configuração de FC de quatro nós

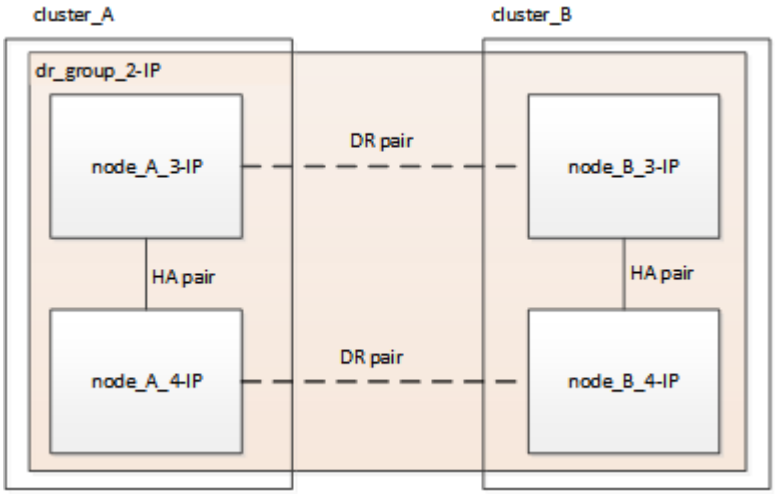
O processo de transição começa com uma configuração MetroCluster FC de quatro nós íntegra.



Os novos nós IP do MetroCluster são adicionados como um segundo grupo de DR.

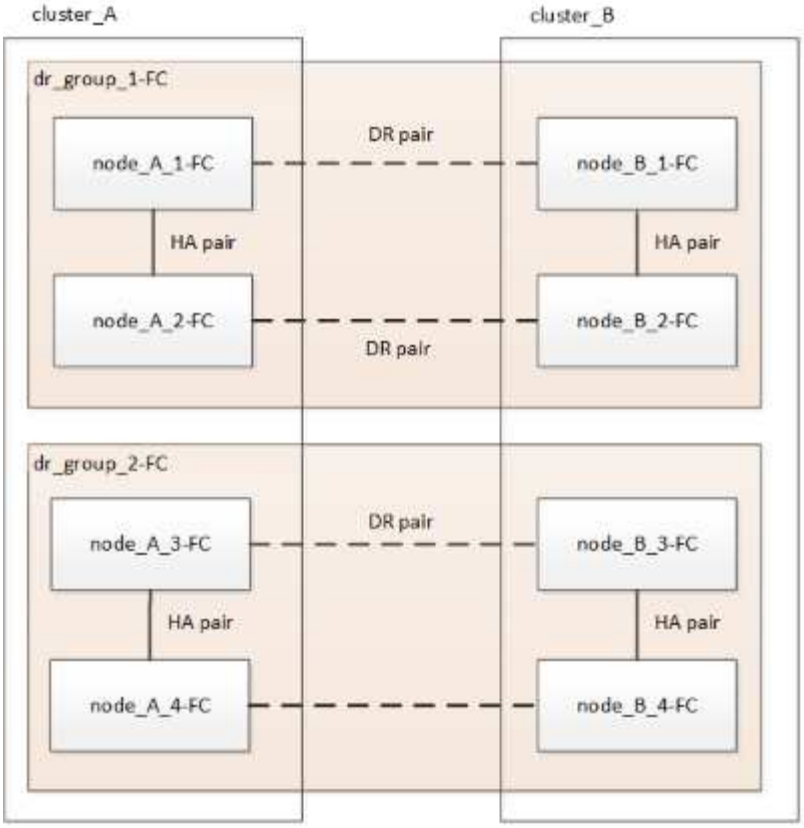


Os dados são transferidos do antigo grupo de DR para o novo grupo de DR. Depois, os nós antigos e o storage são removidos da configuração e desativados. O processo termina com uma configuração IP MetroCluster de quatro nós.

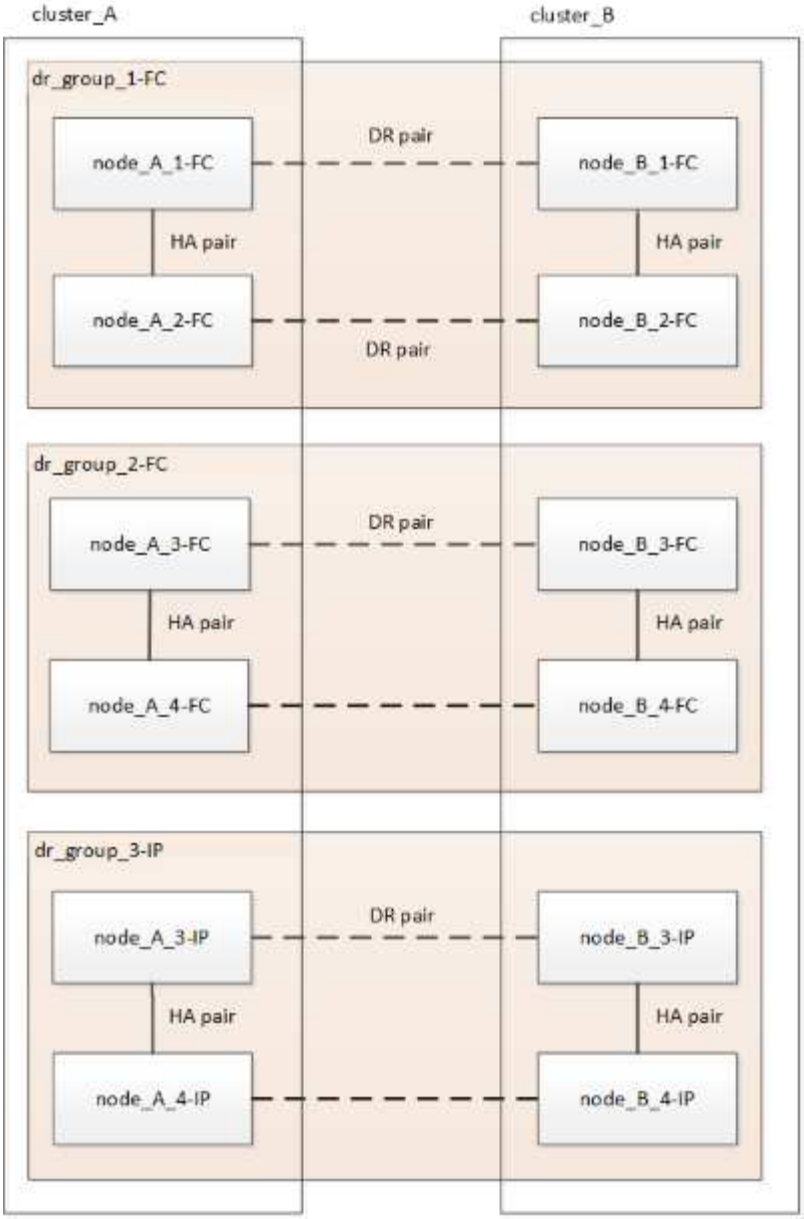


Fluxo de trabalho de transição de configuração de FC de oito nós

O processo de transição começa com uma configuração saudável de MetroCluster FC de oito nós.

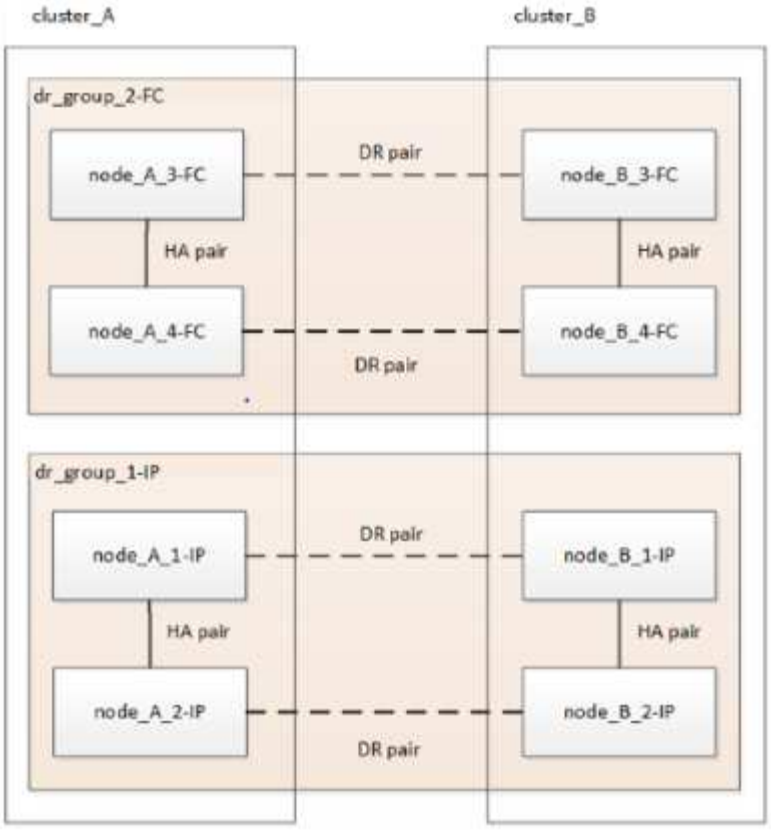


Os novos nós IP do MetroCluster são adicionados como um terceiro grupo de DR.

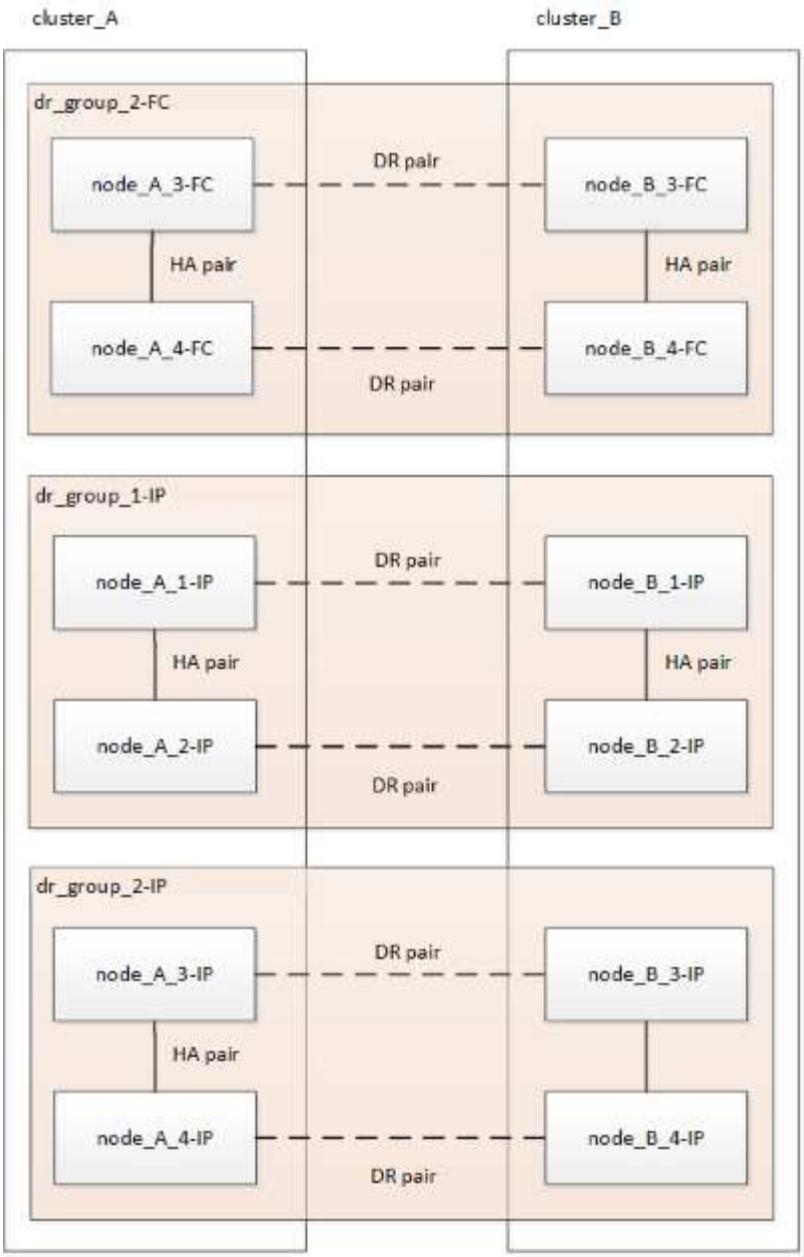


Os dados são transferidos do DR_Group_1-FC para DR_Group_1-IP e, em seguida, os nós antigos e seu storage são removidos da configuração e desativados.

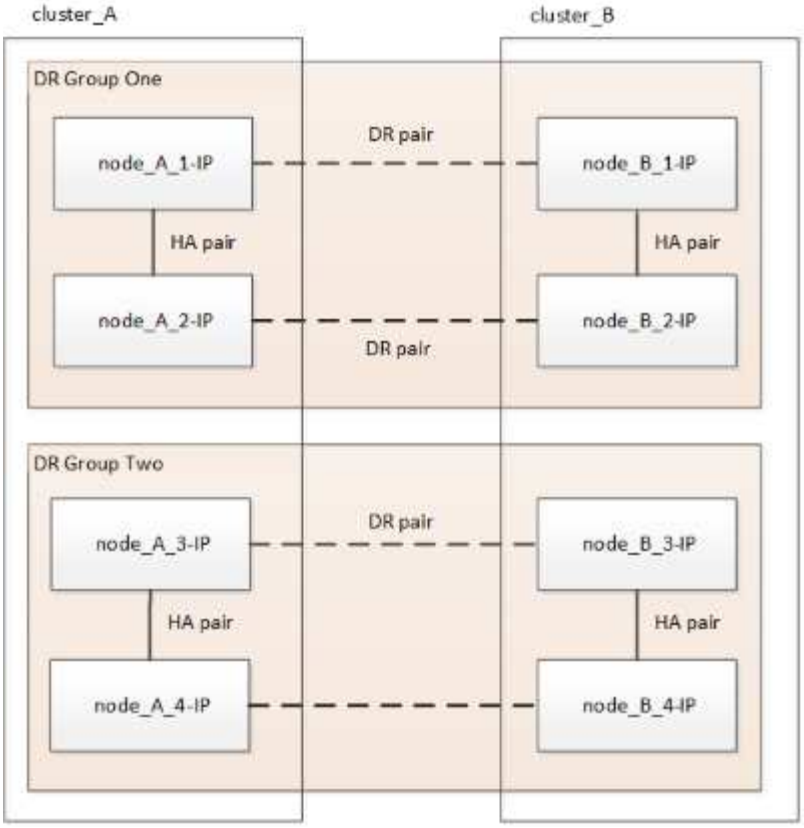
Se você quiser fazer a transição de uma configuração FC de oito nós para uma configuração IP de quatro nós, será necessário fazer a transição de todos os dados em DR_Group_1-FC e DR_Group_2-FC para o novo grupo de DR IP (DR_Group_1-IP). Em seguida, é possível desativar os dois grupos de RD FC. Após a remoção dos grupos de DR FC, o processo termina com uma configuração IP MetroCluster de quatro nós.



Adicione os nós IP restantes do MetroCluster à configuração do MetroCluster existente. Repita o processo para transferir dados dos nós DR_Group_2-FC para os nós DR_Group_2-IP.

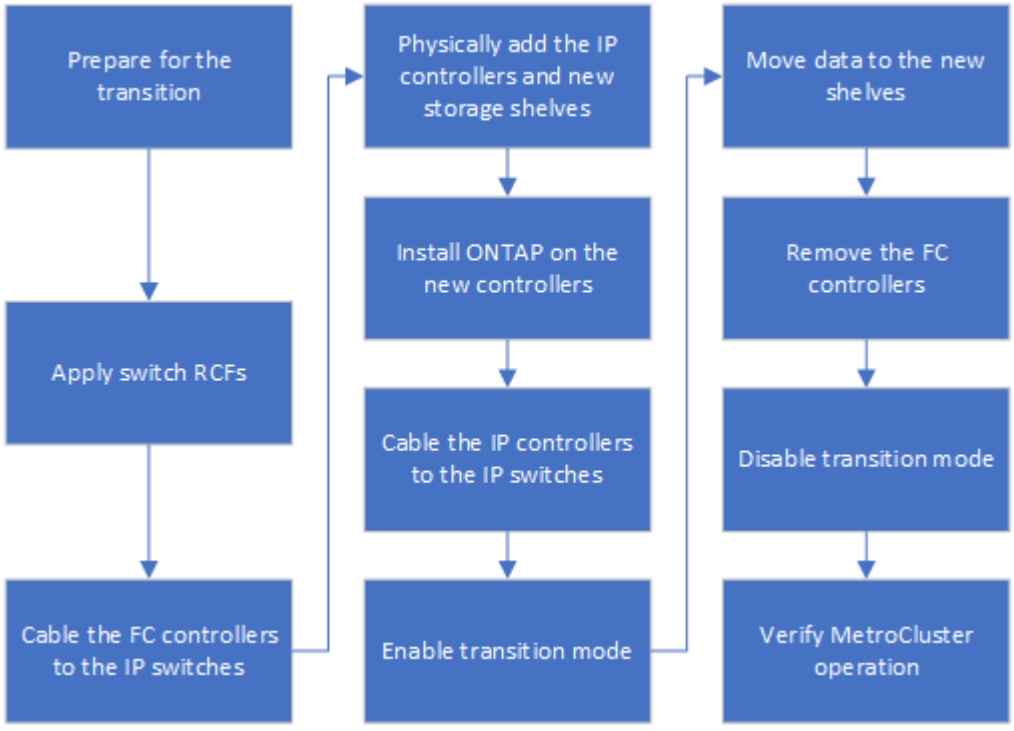


Depois de remover DR_Group_2-FC, o processo termina com uma configuração IP MetroCluster de oito nós.



Fluxo de trabalho do processo de transição

Você usará o fluxo de trabalho a seguir para fazer a transição da configuração do MetroCluster.



Considerações para switches IP

Você deve garantir que os switches IP são suportados. Se o modelo de switch existente

for suportado pela configuração original do MetroCluster FC e pela nova configuração IP do MetroCluster, você poderá reutilizar os switches existentes.

Interrutores suportados

Você deve usar switches fornecidos pelo NetApp.

- O uso de switches compatíveis com MetroCluster (switches que não são validados e fornecidos pelo NetApp) não é suportado para transição.
- Os switches IP devem ser suportados como um switch de cluster pela configuração MetroCluster FC e pela configuração MetroCluster IP.
- Os switches IP podem ser reutilizados na nova configuração IP do MetroCluster se o MetroCluster FC for um cluster comutado e os switches do cluster IP forem suportados pela configuração IP do MetroCluster.
- Os novos switches IP geralmente são usados nos seguintes casos:
  - O MetroCluster FC é um cluster sem switch, portanto, novos switches são necessários.
  - O MetroCluster FC é um cluster comutado, mas os switches IP existentes não são suportados na configuração IP do MetroCluster.
  - Você deseja usar diferentes switches para a configuração IP do MetroCluster.

Consulte o *NetApp Hardware Universe* para obter informações sobre o modelo da plataforma e suporte ao switch.

"NetApp Hardware Universe"

Operações de switchover, recuperação e switchback durante a transição sem interrupções

Dependendo da etapa do processo de transição, as operações de switchover, recuperação e switchback do MetroCluster usam o fluxo de trabalho MetroCluster FC ou MetroCluster IP.

A tabela a seguir mostra quais fluxos de trabalho são usados em diferentes estágios do processo de transição. Em alguns estágios, o switchover e o switchback não são suportados.

- No fluxo de trabalho do MetroCluster FC, as etapas de switchover, recuperação e switchback são usadas por uma configuração de MetroCluster FC.
- No fluxo de trabalho IP do MetroCluster, as etapas de comutação, recuperação e switchback são aquelas usadas por uma configuração IP do MetroCluster.
- No fluxo de trabalho unificado, quando ambos os nós FC e IP são configurados, as etapas dependem se NSO ou USO é executado. Os detalhes são mostrados na tabela.

Para obter informações sobre os workflows de MetroCluster FC e IP para switchover, recuperação e switchback, "Compreender a proteção de dados e a recuperação de desastres da MetroCluster"consulte .

O switchover não planejado automático não está disponível durante o processo de transição.

Fase de transição	O switchover negociado usa este fluxo de trabalho…	O switchover não planejado usa esse fluxo de trabalho…

Antes que os nós IP do MetroCluster se juntem ao cluster	FC MetroCluster	FC MetroCluster
Depois que os nós IP do MetroCluster se conetarem ao cluster, antes que o `metrocluster configure` comando seja executado	Não suportado	FC MetroCluster
Após o `metrocluster configure` comando ter sido emitido. A movimentação de volume pode estar em andamento.	Unificado: Todos os nós do local remoto permanecem ativos e a recuperação é feita automaticamente	Unificado: • Agregados espelhados de propriedade do nó MetroCluster FC são espelhados se o storage estiver acessível, todos os outros são degradados após o switchover. • Todos os nós do local remoto são capazes de inicializar. • Os `heal aggregate` comandos e `heal root` devem ser executados manualmente.
Os nós FC do MetroCluster não foram configurados.	Não suportado	IP MetroCluster
O `cluster unjoin` comando foi executado nos nós MetroCluster FC.	IP MetroCluster	IP MetroCluster

Mensagens de alerta e suporte de ferramentas durante a transição

Você pode notar mensagens de alerta durante a transição. Esses alertas podem ser ignorados com segurança. Além disso, algumas ferramentas não estão disponíveis durante a transição.

- OS ARS podem alertar durante a transição.

  Esses alertas podem ser ignorados e devem desaparecer assim que a transição for concluída.

- O OnCommand Unified Manager pode alertar durante a transição.

  Esses alertas podem ser ignorados e devem desaparecer assim que a transição for concluída.

- O Config Advisor não é suportado durante a transição.
- O System Manager não é suportado durante a transição.

Exemplo de nomeação neste procedimento

Este procedimento usa nomes de exemplo em todo o para identificar os grupos de DR, nós e switches envolvidos.

Grupos DR	Cluster_A no site_A	Cluster_B no local_B
DR_Group_1-FC	• Node_A_1-FC • Node_A_2-FC	• Nó_B_1-FC • Nó_B_2-FC
DR_Group_2-IP	• Node_A_3-IP • Node_A_4-IP	• Node_B_3-IP • Node_B_4-IP
Interrutores	Switches iniciais (se a configuração conetada à malha:) • Switch_A_1-FC • Switch_A_2-FC Switches IP MetroCluster: • Switch_A_1-IP • Switch_A_2-IP	Switches iniciais (se a configuração conetada à malha): • Switch_B_1-FC • Switch_B_2-FC Switches IP MetroCluster: • Switch_B_1-IP • Switch_B_2-IP

Transição das configurações MetroCluster FC para MetroCluster IP

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a transição

1. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:`node run -node node-name sysconfig -a`
   b. Verifique se há alertas de integridade em ambos os clusters: `system health alert show`
   c. Confirme a configuração do MetroCluster e se o modo operacional está normal: `metrocluster show`
   d. Execute uma verificação MetroCluster: `metrocluster check run`
   e. Apresentar os resultados da verificação MetroCluster: `metrocluster check show`
   f. Verifique se existem alertas de estado nos interrutores (se presentes): `storage switch show`
   g. Execute o Config Advisor.

      "NetApp Downloads: Config Advisor"

   h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.
2. Verifique se o cluster está em bom estado: `cluster show`

```
cluster_A::> cluster show
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1_FC    true    true          false
node_A_2_FC    true    true          false

cluster_A::>
```

3. Verifique se todas as portas do cluster estão ativas: `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verifique se todas as LIFs de cluster estão ativas e operacionais: `network interface show -vserver cluster`

   Cada LIF de cluster deve exibir "true" para "is Home" e "up/up" para "Status Admin/Oper".

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A-1_FC_clus1
                       up/up      169.254.209.69/16  node_A-1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verifique se a reversão automática está ativada em todas as LIFs do cluster: `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1_FC_clus1
                        true
           node_A_1_FC_clus2
                        true
           node_A_2_FC_clus1
                        true
           node_A_2_FC_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Remoção da configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes da transição.

1. Remova a configuração existente do MetroCluster do software tiebreaker.

   "Remoção das configurações do MetroCluster"

2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Gerando e aplicando RCFs aos novos switches IP

Se você estiver usando novos switches IP para a configuração IP do MetroCluster, você deverá configurar os switches com um arquivo RCF personalizado.

Esta tarefa é necessária se você estiver usando novos switches.

Se estiver a utilizar comutadores existentes, avance para "Mover as conexões do cluster local".

1. Instale e coloque em rack os novos switches IP.
2. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

Siga as etapas na seção do fornecedor de switch no "Instalação e configuração IP do MetroCluster"

- "Redefinindo o switch IP Broadcom para os padrões de fábrica"
- "Repor as predefinições de fábrica do interrutor IP do Cisco"

3. Atualize o firmware do switch para uma versão suportada, se necessário.
4. Use a ferramenta gerador RCF para criar o arquivo RCF dependendo do fornecedor do switch e dos modelos de plataforma e, em seguida, atualizar os switches com o arquivo.

   Siga as etapas na seção do fornecedor do switch em *Instalação e Configuração do IP do MetroCluster*.

   "Instalação e configuração IP do MetroCluster"

   - "Download e instalação dos arquivos Broadcom IP RCF"
   - "Transferir e instalar os ficheiros Cisco IP RCF"

Mova as conexões do cluster local

É necessário mover as interfaces de cluster da configuração MetroCluster FC para os switches IP.

Mova as conexões de cluster nos nós de FC do MetroCluster

É necessário mover as conexões de cluster nos nós FC do MetroCluster para os switches IP. As etapas dependem se você está usando os switches IP existentes ou se você está usando novos switches IP.

Você deve executar esta tarefa em ambos os sites do MetroCluster.

Quais conexões mover

A tarefa a seguir assume um módulo de controlador usando duas portas para as conexões do cluster. Alguns modelos de módulo de controlador usam quatro ou mais portas para a conexão de cluster. Nesse caso, para os fins deste exemplo, as portas são divididas em dois grupos, alternando portas entre os dois grupos

A tabela a seguir mostra as portas de exemplo usadas nesta tarefa.

Número de ligações do grupo de instrumentos no módulo do controlador	Portas do Grupo A	Portas do grupo B.
Dois	e0a	e0b
Quatro	e0a, e0c	e0b, e0d

- As portas do Grupo A conetam-se ao switch local switch_x_1-IP.
- As portas do grupo B se conetam ao switch local switch switch_x_2-IP.

A tabela a seguir mostra a quais portas de switch os nós FC se conetam. Para o switch BES-53248 Broadcom, o uso da porta depende do modelo dos nós IP do MetroCluster.

Modelo do interrutor	Modelo de nó IP MetroCluster	Porta(s) do switch	Liga-se a.
Cisco 3132Q-V, 3232C ou 9336C-FX2	Qualquer	5	Interface de cluster local no nó FC
		6	Interface de cluster local no nó FC
Broadcom BES-53248	FAS500f/A250	1 - 6	Interface de cluster local no nó FC
	FAS8200/A300	3, 4, 9, 10, 11, 12	Interface de cluster local no nó FC
	FAS8300/A400/FAS8700	1 - 6	Interface de cluster local no nó FC

Mover as conexões do cluster local quando usar novos switches IP

Se você estiver usando novos switches IP, será necessário mover fisicamente as conexões de cluster dos nós FC do MetroCluster existentes para os novos switches.

1. Mova as conexões de cluster do grupo de nós FC MetroCluster A para os novos switches IP.

   Use as portas descritas em Quais conexões mover.

   a. Desconete todas as portas do Grupo A do switch ou, se a configuração do MetroCluster FC for um cluster sem switch, desconete-as do nó do parceiro.
   b. Desconete as portas do Grupo A do node_A_1-FC e node_A_2-FC.
   c. Conete as portas do Grupo A de node_A_1-FC às portas do switch para o nó FC no switch_A_1-IP
   d. Conete as portas do Grupo A de node_A_2-FC às portas do switch para o nó FC no switch_A_1-IP
2. Verifique se todas as portas do cluster estão ativas:

```
network port show -ipspace Cluster
```

```
cluster_A::*> network port show -ipspace Cluster

Node: node_A_1-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::*>
```

3. Verifique se os links inter-switch (ISLs) entre sites estão ativos e se os canais de porta estão operacionais:

   `show interface brief`

   No exemplo a seguir, as portas ISL "eth1/15" para "eth1/20" são configuradas como "Po10" para o link do local remoto e "eth1/7" para "eth1/8" são configuradas como "PO1" para o cluster local ISL. O estado de "eth1/15" a "eth1/20", "eth1/7" a "eth1/8", "Po10" e "PO1" deve ser "para cima".

```
IP_switch_A_1# show interface brief

--------------------------------------------------------------------
Port   VRF          Status   IP Address        Speed      MTU
--------------------------------------------------------------------
mgmt0  --            up        100.10.200.20    1000      1500
--------------------------------------------------------------------------------
--------
Ethernet     VLAN   Type Mode    Status     Reason              Speed
Port
Interface                                    Ch #
--------------------------------------------------------------------------------
--------

...
```

```
Eth1/7        1     eth  trunk    up        none                100G(D)
1
Eth1/8        1     eth  trunk    up        none                100G(D)
1

...

Eth1/15       1     eth  trunk    up        none                100G(D)
10
Eth1/16       1     eth  trunk    up        none                100G(D)
10
Eth1/17       1     eth  trunk    up        none                100G(D)
10
Eth1/18       1     eth  trunk    up        none                100G(D)
10
Eth1/19       1     eth  trunk    up        none                100G(D)
10
Eth1/20       1     eth  trunk    up        none                100G(D)
10

--------------------------------------------------------------------------
--------
Port-channel VLAN  Type Mode   Status   Reason         Speed    Protocol
Interface
--------------------------------------------------------------------------
--------
Po1          1     eth  trunk   up      none            a-100G(D) lacp
Po10         1     eth  trunk   up      none            a-100G(D) lacp
Po11         1     eth  trunk   down    No operational  auto(D)   lacp
                                        members
IP_switch_A_1#
```

4. Verifique se todas as interfaces são exibidas verdadeiras na coluna "is Home":

   `network interface show -vserver cluster`

   Isso pode levar vários minutos para ser concluído.

```
cluster_A::*> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1-FC_clus2
                       up/up      169.254.49.125/16  node_A_1-FC   e0b
true
            node_A_2-FC_clus1
                       up/up      169.254.47.194/16  node_A_2-FC   e0a
true
            node_A_2-FC_clus2
                       up/up      169.254.19.183/16  node_A_2-FC   e0b
true

4 entries were displayed.

cluster_A::*>
```

5. Execute as etapas acima em ambos os nós (node_A_1-FC e node_A_2-FC) para mover as portas do grupo B das interfaces de cluster.
6. Repita as etapas acima no cluster de parceiros ""cluster_B"".

Mover as conexões do cluster local ao reutilizar os switches IP existentes

Se estiver a reutilizar os comutadores IP existentes, tem de atualizar o firmware, reconfigurar os comutadores com os RCFs (Reference Configure Files) corretos e mover as ligações para as portas corretas, um switch de cada vez.

Essa tarefa só será necessária se os nós FC estiverem conetados a switches IP existentes e você estiver reutilizando os switches.

1. Desconete as conexões do cluster local que se conetam ao switch_A_1_IP
   a. Desconete as portas do Grupo A do switch IP existente.
   b. Desconete as portas ISL no switch_A_1_IP.

      Você pode ver as instruções de instalação e configuração da plataforma para ver o uso da porta do cluster.

      "Sistemas AFF A320: Instalação e configuração"

"Instruções de instalação e configuração dos sistemas AFF A220/FAS2700"

"Instruções de instalação e configuração de sistemas AFF A800"

"Instruções de instalação e configuração de sistemas AFF A300"

"Instruções de instalação e configuração de sistemas FAS8200"

2. Reconfigure switch_A_1_IP usando arquivos RCF gerados para a combinação e transição da sua plataforma.

   Siga as etapas no procedimento para o fornecedor do switch em *Instalação e Configuração do IP do MetroCluster*:

   "Instalação e configuração IP do MetroCluster"

   a. Se necessário, transfira e instale o novo firmware do switch.

      Você deve usar o firmware mais recente suportado pelos nós IP do MetroCluster.

      - "Download e instalação do software Broadcom switch EFOS"
      - "Transferir e instalar o software Cisco switch NX-os"

   b. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.
      - "Redefinindo o switch IP Broadcom para os padrões de fábrica" **
      - "Repor as predefinições de fábrica do interrutor IP do Cisco"

   c. Baixe e instale o arquivo RCF IP, dependendo do fornecedor do switch.
      - "Download e instalação dos arquivos Broadcom IP RCF"
      - "Transferir e instalar os ficheiros Cisco IP RCF"

3. Reconecte as portas do Grupo A ao switch_A_1_IP.

   Use as portas descritas em Quais conexões mover.

4. Verifique se todas as portas do cluster estão ativas:

   ```
   network port show -ipspace cluster
   ```

```
Cluster-A::*> network port show -ipspace cluster

Node: node_A_1_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

5. Verifique se todas as interfaces estão em sua porta inicial:

   `network interface show -vserver Cluster`

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

6. Repita todos os passos anteriores no switch_A_2_IP.
7. Volte a ligar as portas ISL do cluster local.
8. Repita as etapas acima no site_B para o switch B_1_IP e o switch B_2_IP.
9. Ligue os ISLs remotos entre os locais.

Verificar se as conexões do cluster são movidas e o cluster está funcionando

Para garantir que há conetividade adequada e que a configuração esteja pronta para prosseguir com o processo de transição, você deve verificar se as conexões do cluster são movidas corretamente, os switches do cluster são reconhecidos e o cluster está em bom estado.

1. Verifique se todas as portas do cluster estão ativas e em execução:

   ```
   network port show -ipspace Cluster
   ```

```
Cluster-A::*> network port show -ipspace Cluster

Node: Node-A-1-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: Node-A-2-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

2. Verifique se todas as interfaces estão em sua porta inicial:

   `network interface show -vserver Cluster`

   Isso pode levar vários minutos para ser concluído.

   O exemplo a seguir mostra que todas as interfaces são verdadeiras na coluna "is Home".

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            Node-A-1_FC_clus1
                       up/up      169.254.209.69/16  Node-A-1_FC   e0a
true
            Node-A-1-FC_clus2
                       up/up      169.254.49.125/16  Node-A-1-FC   e0b
true
            Node-A-2-FC_clus1
                       up/up      169.254.47.194/16  Node-A-2-FC   e0a
true
            Node-A-2-FC_clus2
                       up/up      169.254.19.183/16  Node-A-2-FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

3. Verifique se ambos os switches IP locais são descobertos pelos nós:

   `network device-discovery show -protocol cdp`

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
Node-A-1-FC
           /cdp
            e0a    Switch-A-3-IP             1/5/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/5/1             N3K-
C3232C
Node-A-2-FC
           /cdp
            e0a    Switch-A-3-IP             1/6/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/6/1             N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. No switch IP, verifique se os nós IP do MetroCluster foram descobertos por ambos os switches IP locais:

   `show cdp neighbors`

   Tem de executar este passo em cada interrutor.

   Este exemplo mostra como verificar se os nós são descobertos no Switch-A-3-IP.

```
(Switch-A-3-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0a
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0a
Switch-A-4-IP(FDO220329A4)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-4-IP(FDO220329A4)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-3-IP(FDO220329B3)
                    Eth1/20        173    R S I s   N3K-C3232C
Eth1/20
Switch-B-3-IP(FDO220329B3)
                    Eth1/21        173    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-3-IP)#
```

Este exemplo mostra como verificar se os nós são descobertos no Switch-A-4-IP.

```
(Switch-A-4-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0b
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0b
Switch-A-3-IP(FDO220329A3)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-3-IP(FDO220329A3)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-4-IP(FDO220329B4)
                    Eth1/20        169    R S I s   N3K-C3232C
Eth1/20
Switch-B-4-IP(FDO220329B4)
                    Eth1/21        169    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP)#
```

Preparação dos controladores IP MetroCluster

Você deve preparar os quatro novos nós IP do MetroCluster e instalar a versão correta do ONTAP.

Esta tarefa deve ser executada em cada um dos novos nós:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

Nestas etapas, você limpa a configuração nos nós e limpa a região da caixa de correio em novas unidades.

1. Rack os novos controladores para a configuração IP do MetroCluster.

   Os nós de FC do MetroCluster (node_A_x-FC e node_B_x-FC) permanecem cabeados no momento.

2. Faça o cabeamento dos nós IP do MetroCluster aos switches IP, conforme mostrado na "Cabeamento dos switches IP".

3. Configure os nós IP do MetroCluster usando as seguintes seções:
   a. "Reúna as informações necessárias"
   b. "Restaure os padrões do sistema em um módulo do controlador"
   c. "Verifique o estado ha-config dos componentes"
   d. "Atribuir manualmente unidades para o pool 0 (ONTAP 9.4 e posterior)"
4. No modo Manutenção, emita o comando halt para sair do modo Manutenção e, em seguida, emita o comando boot_ONTAP para inicializar o sistema e chegar à configuração do cluster.

   Não conclua o assistente de cluster ou o assistente de nó neste momento.
5. Repita estas etapas nos outros nós IP do MetroCluster.

Configure o MetroCluster para a transição

Para preparar a configuração para a transição, adicione os novos nós à configuração existente do MetroCluster e, em seguida, mova os dados para os novos nós.

Enviar uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Para evitar a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a manutenção está em andamento:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   "manutenção-janela-em-horas" especifica o comprimento da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```
2. Repita o comando no cluster de parceiros.

Ativar o modo de transição e desativar o cluster HA

Você deve habilitar o modo de transição do MetroCluster para permitir que os nós antigos e novos operem juntos na configuração do MetroCluster e desabilitar o HA do cluster.

1. Ativar transição:
   a. Mude para o nível de privilégio avançado:

      ```
      set -privilege advanced
      ```

b. Ativar modo de transição:

```
metrocluster transition enable -transition-mode non-disruptive
```

Execute este comando apenas em um cluster.

```
cluster_A::*> metrocluster transition enable -transition-mode non-
disruptive

Warning: This command enables the start of a "non-disruptive"
MetroCluster
         FC-to-IP transition. It allows the addition of hardware for
another DR
         group that uses IP fabrics, and the removal of a DR group that
uses FC
         fabrics. Clients will continue to access their data during a
         non-disruptive transition.

         Automatic unplanned switchover will also be disabled by this
command.
Do you want to continue? {y|n}: y

cluster_A::*>
```

a. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

2. Verifique se a transição está ativada nos dois clusters.

```
cluster_A::> metrocluster transition show-mode
Transition Mode

non-disruptive

cluster_A::*>


cluster_B::*> metrocluster transition show-mode
Transition Mode

non-disruptive

Cluster_B::>
```

3. Desative o cluster HA.

   Você deve executar esse comando em ambos os clusters.

```
cluster_A::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_A::*>


cluster_B::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_B::*>
```

4. Verifique se a HA do cluster está desativada.

   Você deve executar esse comando em ambos os clusters.

```
cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>
```

Unindo os nós IP do MetroCluster aos clusters

Você deve adicionar os quatro novos nós IP do MetroCluster à configuração existente do MetroCluster.

Sobre esta tarefa

Você deve executar essa tarefa em ambos os clusters.

Passos

1. Adicione os nós IP do MetroCluster à configuração do MetroCluster existente.
   a. Junte o primeiro nó IP do MetroCluster (node_A_3-IP) à configuração FC do MetroCluster existente.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.
```

```
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter autosupport modify -support
disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:

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


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Junte o segundo nó IP do MetroCluster (node_A_4-IP) à configuração FC do MetroCluster existente.

2. Repita estas etapas para unir node_B_3-IP e node_B_4-IP ao cluster_B.

Configurando LIFs entre clusters, criando interfaces MetroCluster e espelhando agregados de raiz

Você deve criar LIFs de peering de cluster, criar as interfaces MetroCluster nos novos nós IP do MetroCluster.

Sobre esta tarefa

A porta inicial usada nos exemplos é específica da plataforma. Você deve usar a porta inicial apropriada específica da plataforma do nó IP do MetroCluster.

Passos

1. Nos novos nós IP do MetroCluster, "Configurar as LIFs entre clusters".
2. Em cada site, verifique se o peering de cluster está configurado:

   ```
   cluster peer show
   ```

   O exemplo a seguir mostra a configuração de peering de cluster no cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   O exemplo a seguir mostra a configuração de peering de cluster no cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A 1-80-000011 Available ok
   ```

3. Configure o grupo de DR para os nós IP do MetroCluster:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   ```
   cluster_A::> metrocluster configuration-settings dr-group create
   -partner-cluster
   cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
   [Job 259] Job succeeded: DR Group Create is successful.
   cluster_A::>
   ```

4. Verifique se o grupo de DR foi criado.

   ```
   metrocluster configuration-settings dr-group show
   ```

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
2           cluster_A
                                       node_A_3-IP        node_B_3-IP
                                       node_A_4-IP        node_B_4-IP
            cluster_B
                                       node_B_3-IP        node_A_3-IP
                                       node_B_4-IP        node_A_4-IP

4 entries were displayed.

cluster_A::>
```

Você notará que o grupo de DR para os nós FC MetroCluster antigos (Grupo de DR 1) não está listado quando você executa o `metrocluster configuration-settings dr-group show` comando.

Você pode usar `metrocluster node show` o comando em ambos os sites para listar todos os nós.

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
      cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
2     cluster_A
              node_A_3-IP      ready to configure
                                                 -         -
              node_A_4-IP      ready to configure
                                                 -         -

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
      cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
2     cluster_B
              node_B_3-IP      ready to configure
                                                 -         -
              node_B_4-IP      ready to configure
                                                 -         -
```

5. Configure as interfaces IP do MetroCluster para os nós IP do MetroCluster recém-ingressados:

   `metrocluster configuration-settings interface create -cluster-name`

   Consulte "Configuração e conexão das interfaces IP do MetroCluster" para obter considerações ao configurar as interfaces IP.

   Você pode configurar as interfaces IP do MetroCluster a partir de qualquer cluster.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verifique se as interfaces IP do MetroCluster são criadas:

```
metrocluster configuration-settings interface show
```

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
2     cluster_A
             node_A_3-IP
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-IP
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Conete as interfaces IP do MetroCluster:

```
metrocluster configuration-settings connection connect
```

Esse comando pode levar vários minutos para ser concluído.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verifique se as conexões estão corretamente estabelecidas:

`metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_3-IP**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
```

```
                     172.17.26.11    172.17.26.12    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.10    HA Partner
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.13    DR Partner
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                   Source          Destination
Group Cluster Node   Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_4-IP
                 Home Port: e1a
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_3-IP
                 Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
```

```
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.10    DR Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. Verifique a atribuição automática e o particionamento do disco:

   ```
   disk show -pool Pool1
   ```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0                546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3                546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5                546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6                546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7                546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10               546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.
cluster_A::>
```

Em sistemas configurados para Advanced Drive Partitioning (ADP), o tipo de contentor é "compartilhado" em vez de "remoto", como mostrado na saída de exemplo.

10. Espelhar os agregados de raiz:

```
storage aggregate mirror -aggregate aggr0_node_A_3_IP
```

Você deve concluir esta etapa em cada nó IP do MetroCluster.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3_IP

Info: Disks would be added to aggregate "aggr0_node_A_3_IP"on node
"node_A_3-IP"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available for volume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verifique se os agregados raiz estão espelhados:

`storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1_FC
           349.0GB   16.84GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2_FC
           349.0GB   16.84GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3_IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_4_IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-FC
raid_dp,

mirrored,
```

Finalizando a adição dos nós IP do MetroCluster

Você precisa incorporar o novo grupo de DR à configuração do MetroCluster e criar agregados de dados espelhados nos novos nós.

Passos

1. Configure o MetroCluster dependendo se ele tem um único ou vários agregados de dados:

Se a sua configuração do MetroCluster tiver…	Então faça isso…

Vários agregados de dados	A partir do prompt de qualquer nó, configure o MetroCluster: `metrocluster configure <node-name>` Você deve correr `metrocluster configure` e **não** `metrocluster configure -refresh true`
Um único agregado de dados espelhados	a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado: `set -privilege advanced` Você deve responder `y` quando for solicitado a continuar no modo avançado e você vir o prompt do modo avançado (*>). b. Configure o MetroCluster com o `-allow-with -one-aggregate true` parâmetro: `metrocluster configure -allow-with -one-aggregate true -node-name <node-name>` c. Voltar ao nível de privilégio de administrador: `set -privilege admin`

A prática recomendada é ter vários agregados de dados espelhados. Quando há apenas um agregado espelhado, há menos proteção porque os volumes de metadados estão localizados no mesmo agregado, em vez de em agregados separados.

2. Reinicie cada um dos novos nós:

```
node reboot -node <node_name> -inhibit-takeover true
```

Você não precisa reiniciar os nós em uma ordem específica, mas você deve esperar até que um nó seja totalmente inicializado e todas as conexões sejam estabelecidas antes de reiniciar o próximo nó.

3. Verifique se os nós são adicionados ao grupo de DR:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node-A-1-FC        configured     enabled   normal
              node-A-2-FC        configured     enabled   normal
      Cluster-B
              node-B-1-FC        configured     enabled   normal
              node-B-2-FC        configured     enabled   normal
2     cluster_A
              node-A-3-IP        configured     enabled   normal
              node-A-4-IP        configured     enabled   normal
      Cluster-B
              node-B-3-IP        configured     enabled   normal
              node-B-4-IP        configured     enabled   normal
8 entries were displayed.

cluster_A::>
```

4. Crie agregados de dados espelhados em cada um dos novos nós MetroCluster:

   `storage aggregate create -aggregate aggregate-name -node node-name -diskcount no-of-disks -mirror true`

   > Você deve criar pelo menos um agregado de dados espelhados por local. Recomenda-se ter dois agregados de dados espelhados por local em nós IP do MetroCluster para hospedar os volumes MDV. No entanto, um único agregado por local é suportado (mas não recomendado). É aceitável que um site do MetroCluster tenha um único agregado de dados espelhados e o outro site tenha mais de um agregado de dados espelhados.

   O exemplo a seguir mostra a criação de um agregado em node_A_3-IP.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_3-
IP -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_3-IP" would be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
```

```
Size
          ---------- ------------------------ ---------- --------
--------
          dparity    5.10.15                  SAS                -
-
          parity     5.10.16                  SAS                -
-
          data       5.10.17                  SAS         546.9GB
547.1GB
          data       5.10.18                  SAS         546.9GB
558.9GB
          data       5.10.19                  SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                     Type           Size
Size
          ---------- ------------------------ ---------- --------
--------
          dparity    4.20.17                  SAS                -
-
          parity     4.20.14                  SAS                -
-
          data       4.20.18                  SAS         546.9GB
547.1GB
          data       4.20.19                  SAS         546.9GB
547.1GB
          data       4.20.16                  SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

5. Verifique se todos os nós no cluster estão íntegros:

   `cluster show`

   A saída deve ser exibida `true` para o `health` campo para todos os nós.

6. Confirme se o takeover é possível e os nós estão conectados executando o seguinte comando em ambos os clusters:

   `storage failover show`

   ```
   cluster_A::> storage failover show
                                       Takeover
   Node           Partner              Possible    State Description
   -------------- -------------------- ---------   ------------------
   Node_FC_1      Node_FC_2              true      Connected to Node_FC_2
   Node_FC_2      Node_FC_1              true      Connected to Node_FC_1
   Node_IP_1      Node_IP_2              true      Connected to Node_IP_2
   Node_IP_2      Node_IP_1              true      Connected to Node_IP_1
   ```

7. Confirme se todos os discos conetados aos nós IP do MetroCluster recém-ingressados estão presentes:

   `disk show`

8. Verifique a integridade da configuração do MetroCluster executando os seguintes comandos:
   a. `metrocluster check run`
   b. `metrocluster check show`
   c. `metrocluster interconnect mirror show`
   d. `metrocluster interconnect adapter show`
9. Mova os volumes MDV_CRS dos nós antigos para os novos nós no privilégio avançado.
   a. Apresentar os volumes para identificar os volumes MDV:

      Se você tiver um único agregado de dados espelhados por local, mova ambos os volumes MDV para esse único agregado. Se você tiver dois ou mais agregados de dados espelhados, mova cada volume MDV para um agregado diferente.

      O exemplo a seguir mostra os volumes MDV na saída de exibição de volume:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Defina o nível de privilégio avançado:

```
set -privilege advanced
```

c. Mova os volumes MDV, um de cada vez:

```
volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name
```

O exemplo a seguir mostra o comando e a saída para mover MDV_CRS_d6b0b313ff5611e9837100a098544e51_A para agregar data_A3 em node_A_3.

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Use o comando volume show para verificar se o volume MDV foi movido com sucesso:

```
volume show mdv-name
```

A saída seguinte mostra que o volume MDV foi movido com sucesso.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

a. Voltar ao modo de administração:

```
set -privilege admin
```

Mover os dados para as novas gavetas de unidades

Durante a transição, você migra dados dos compartimentos de unidades na configuração MetroCluster FC para a nova configuração MetroCluster IP.

Antes de começar

Você deve criar novos LIFs SAN no destino ou nos nós IP e conectar hosts antes de mover volumes para novos agregados.

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.

a. Emita o seguinte comando: `system node autosupport invoke -node * -type all -message MAINT=end`

b. Repita o comando no cluster de parceiros.

2. Mova os volumes de dados para agregados nas novas controladoras, um volume de cada vez.

   Utilize o procedimento em "Criando um agregado e movendo volumes para os novos nós".

3. Crie SAN LIFs nos nós adicionados recentemente.

   Use o seguinte procedimento "Atualizando caminhos de LUN para os novos nós" em .

4. Verifique se há alguma licença de nó bloqueado nos nós FC, se houver, elas precisam ser adicionadas aos nós recém-adicionados.

   Use o seguinte procedimento "Adição de licenças com bloqueio de nó" em .

5. Migrar os LIFs de dados.

   Use o procedimento em "Mover LIFs de dados que não são SAN e LIFs de gerenciamento de cluster para os novos nós", mas **não**, execute as duas últimas etapas para migrar LIFs de gerenciamento de cluster.

- Você não pode migrar um LIF usado para operações de descarga de cópia com o VMware vStorage APIs for Array Integration (VAAI).
- Depois de concluir a transição dos nós do MetroCluster do FC para o IP, talvez seja necessário mover as conexões do host iSCSI para os novos nós. Consulte "Movimentação de hosts iSCSI Linux do MetroCluster FC para nós IP MetroCluster."

Remoção das controladoras MetroCluster FC

Você deve executar tarefas de limpeza e remover os módulos antigos do controlador da configuração do MetroCluster.

1. Para evitar a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a manutenção está em andamento.

   a. Emita o seguinte comando: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      maintenance-window-in-hours especifica a duração da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repita o comando no cluster de parceiros.

2. Identificar os agregados hospedados na configuração de FC MetroCluster que precisam ser excluídos.

   Neste exemplo, os seguintes agregados de dados são hospedados pelo cluster_B do MetroCluster FC e precisam ser excluídos: aggr_data_A1 e aggr_data_A2.

Você precisa executar as etapas para identificar, off-line e excluir os agregados de dados em ambos os clusters. O exemplo é apenas para um cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.83GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.02TB    0% online       0 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.02TB    0% online       0 node_A_2-FC
raid_dp,
```

```
mirrored,

normal
aggr_data_a3
            1.37TB    1.35TB    1% online       3 node_A_3-IP
raid_dp,

mirrored,

normal
aggr_data_a4
            1.25TB    1.24TB    1% online       2 node_A_4-IP
raid_dp,

mirrored,

normal
8 entries were displayed.

cluster_B::>
```

3. Verifique se os agregados de dados nos nós FC têm quaisquer volumes MDV_aud e exclua-os antes de excluir os agregados.

   Você deve excluir os volumes MDV_aud porque eles não podem ser movidos.

4. Tire cada um dos agregados de dados offline e, em seguida, exclua-os:

   a. Coloque o agregado off-line: `storage aggregate offline -aggregate aggregate-name`

      O exemplo a seguir mostra que aggr_data_A1 agregado está sendo colocado off-line:

      ```
      cluster_B::> storage aggregate offline -aggregate aggr_data_a1

      Aggregate offline successful on aggregate: aggr_data_a1
      ```

   b. Eliminar o agregado: `storage aggregate delete -aggregate aggregate-name`

      Você pode destruir o Plex quando solicitado.

      O exemplo a seguir mostra que aggr_data_A1 agregado está sendo excluído.

```
cluster_B::> storage aggregate delete -aggregate aggr_data_a1
Warning: Are you sure you want to destroy aggregate "aggr_data_a1"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

5. Identifique o grupo de DR do MetroCluster FC que precisa ser removido.

   No exemplo a seguir, os nós FC do MetroCluster estão no grupo de DR '1', e este é o grupo de DR que precisa ser removido.

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        configured     enabled   normal
              node_A_2-FC        configured     enabled   normal
      cluster_B
              node_B_1-FC        configured     enabled   normal
              node_B_2-FC        configured     enabled   normal
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_3-IP        configured     enabled   normal
8 entries were displayed.

cluster_B::>
```

6. Mova o LIF de gerenciamento de cluster de um nó MetroCluster FC para um nó MetroCluster IP: `cluster_B::> network interface migrate -vserver svm-name -lif cluster_mgmt -destination-node node-in-metrocluster-ip-dr-group -destination-port available-port`
7. Altere o nó inicial e a porta inicial do LIF de gerenciamento de cluster: `cluster_B::> network interface modify -vserver svm-name -lif cluster_mgmt -service-policy default-management -home-node node-in-metrocluster-ip-dr-group -home-port lif-port`
8. Mova o epsilon de um nó MetroCluster FC para um nó MetroCluster IP:
   a. Identificar qual nó tem atualmente o epsilon: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      true
node_A_2-FC      false
node_A_1-IP      false
node_A_2-IP      false
4 entries were displayed.
```

b. Defina epsilon como false no nó MetroCluster FC (node_A_1-FC): `cluster modify -node fc-node -epsilon false`

c. Defina epsilon como true no nó IP do MetroCluster (node_A_1-IP): `cluster modify -node ip-node -epsilon true`

d. Verifique se o epsilon foi movido para o nó correto: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      false
node_A_2-FC      false
node_A_1-IP      true
node_A_2-IP      false
4 entries were displayed.
```

9. Modifique o endereço IP para o ponto de cluster dos nós IP transicionados para cada cluster:

a. Identifique o peer cluster_A usando o `cluster peer show` comando:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

i. Modifique o endereço IP peer cluster_A:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

b. Identifique o peer cluster_B usando o `cluster peer show` comando:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

i. Modifique o endereço IP peer cluster_B:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

c. Verifique se o endereço IP do peer do cluster está atualizado para cada cluster:

i. Verifique se o endereço IP é atualizado para cada cluster usando o `cluster peer show -instance` comando.

O `Remote Intercluster Addresses` campo nos exemplos a seguir exibe o endereço IP atualizado.

Exemplo para cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_B
                     Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+
Exemplo para cluster_B

```
cluster_B::> cluster peer show -instance

                      Peer Cluster Name: cluster_A
          Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                  Remote Cluster Health: true
                Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                        Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. Em cada cluster, remova o grupo de DR que contém os nós antigos da configuração do MetroCluster FC.

    Você deve executar essa etapa em ambos os clusters, um de cada vez.

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B" to remove the remote nodes in the
DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed ifthe preparation steps are not completed on
the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_B::>
```

11. Verifique se os nós estão prontos para serem removidos dos clusters.

    É necessário executar esta etapa em ambos os clusters.

    Nesse ponto, o `metrocluster node show` comando mostra apenas os nós FC do MetroCluster local e não mostra mais os nós que fazem parte do cluster de parceiros.

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        ready to configure
                                                -         -
              node_A_2-FC        ready to configure
                                                -         -
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_4-IP        configured     enabled   normal
6 entries were displayed.

cluster_B::>
```

12. Desativar o failover de storage para os nós FC do MetroCluster.

    Você deve executar esta etapa em cada nó.

```
cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>
```

13. Desmarque os nós do MetroCluster FC dos clusters: `cluster unjoin -node node-name`

    Você deve executar esta etapa em cada nó.

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC"from the cluster.
You must
         remove the failover partner as well. After the node is removed,
erase
         its configuration and initialize all disks by usingthe "Clean
         configuration and initialize all disks (4)" option from the
boot menu.
Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

14. Desligue os módulos de controlador MetroCluster FC e as gavetas de storage.
15. Desconete e remova os módulos de controlador MetroCluster FC e as gavetas de storage.

Concluir a transição

Para concluir a transição, você deve verificar a operação da nova configuração IP do MetroCluster.

1. Verifique a configuração IP do MetroCluster.

   Você deve executar esta etapa em cada cluster.

   O exemplo a seguir mostra a saída para cluster_A.

```
cluster_A::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_A_1-IP          true    true          true
node_A_2-IP          true    true          false
2 entries were displayed.

cluster_A::>
```

O exemplo a seguir mostra a saída para cluster_B.

```
cluster_B::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_B_1-IP          true    true          true
node_B_2-IP          true    true          false
2 entries were displayed.

cluster_B::>
```

2. Habilitar a HA do cluster e o failover de storage.

   Você deve executar esta etapa em cada cluster.

3. Verifique se a capacidade de HA do cluster está ativada.

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>


cluster_A::> storage  failover show
                             Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1-IP    node_A_2-IP    true     Connected to node_A_2-IP
node_A_2-IP    node_A_1-IP    true     Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. Desativar o modo de transição MetroCluster.

   a. Mude para o nível de privilégio avançado: `set -privilege advanced`

   b. Desativar modo de transição:`metrocluster transition disable`

   c. Voltar ao nível de privilégio de administrador: `set -privilege admin`

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. Verifique se a transição está desativada:`metrocluster transition show-mode`

   Você deve executar essas etapas em ambos os clusters.

```
cluster_A::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_A::>
```

```
cluster_B::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_B::>
```

6. Se você tiver uma configuração de oito nós, repita todo o procedimento a partir de "Prepare-se para a transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP" para cada um dos grupos de RD FC.

Enviar uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a transição, você deve enviar uma mensagem AutoSupport indicando o fim da manutenção, para que a criação automática de casos possa ser retomada.

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.
   a. Emita o seguinte comando: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repita o comando no cluster de parceiros.

Restaurar a monitorização do tiebreaker ou do Mediator

Depois de concluir a transição da configuração do MetroCluster, você pode retomar o monitoramento com o utilitário tiebreaker ou Mediator.

1. Use o procedimento apropriado para sua configuração.

Se você estiver usando…	Use este procedimento
Desempate	"Adição de configurações do MetroCluster"

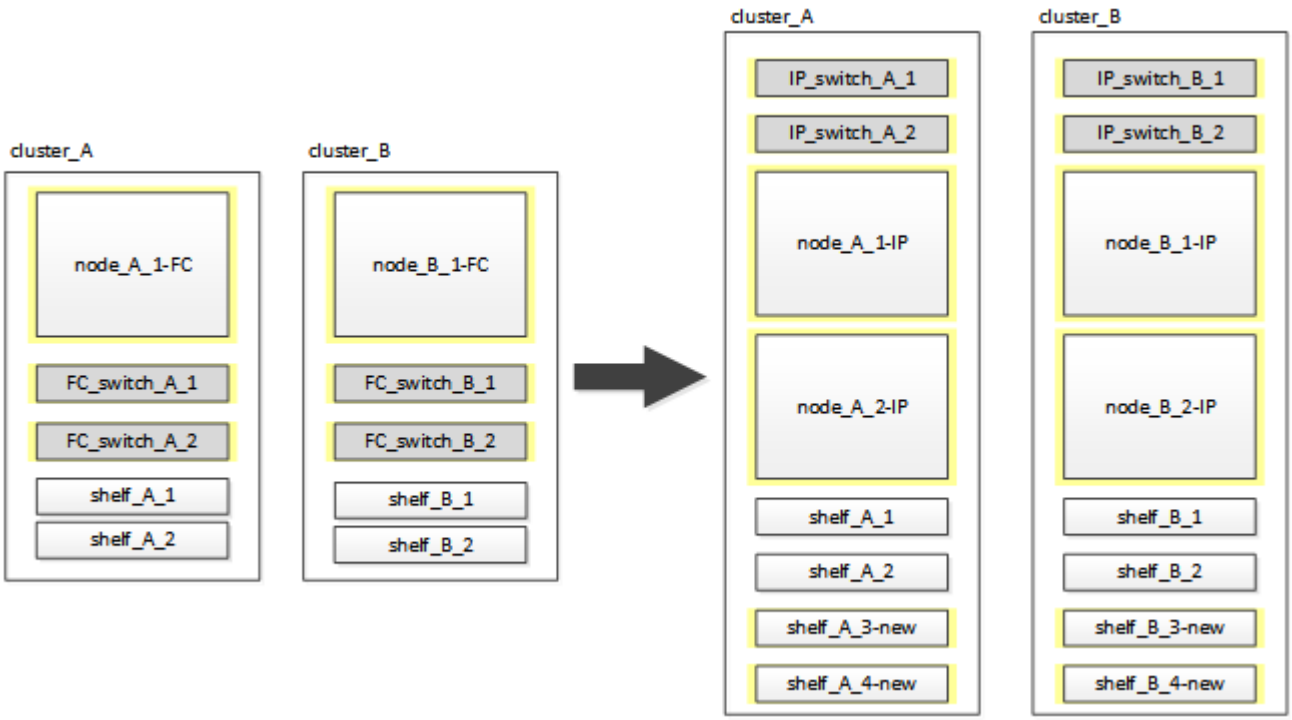
Mediador	"Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster"

Transição de um MetroCluster FC de dois nós para uma configuração IP MetroCluster de quatro nós (ONTAP 9.8 e posterior) sem interrupções.

Transição de um MetroCluster FC de dois nós para uma configuração IP MetroCluster de quatro nós (ONTAP 9.8 e posterior) sem interrupções.

A partir do ONTAP 9.8, você pode migrar workloads e dados de uma configuração MetroCluster FC de dois nós existente para uma nova configuração MetroCluster IP de quatro nós. As gavetas de disco dos nós FC do MetroCluster são movidas para os nós IP.

A ilustração a seguir fornece uma visão simplificada da configuração antes e depois deste procedimento de transição.



- Este procedimento é suportado em sistemas que executam o ONTAP 9.8 e posterior.
- Este procedimento é disruptivo.
- Esse procedimento se aplica apenas a uma configuração de FC MetroCluster de dois nós.

  Se você tiver uma configuração de FC MetroCluster de quatro nós, "Escolhendo seu procedimento de transição"consulte .

- ADP não é suportado na configuração IP MetroCluster de quatro nós criada por este procedimento.

- Você deve atender a todos os requisitos e seguir todas as etapas do procedimento.
- As gavetas de storage existentes são movidas para os novos nós IP do MetroCluster.
- Prateleiras de armazenamento adicionais podem ser adicionadas à configuração, se necessário.

  "Reutilização do compartimento de unidade e requisitos de unidade para uma transição FC para IP disruptiva"Consulte .

Exemplo de nomeação neste procedimento

Este procedimento usa nomes de exemplo em todo o para identificar os grupos de DR, nós e switches envolvidos.

Os nós na configuração original têm o sufixo -FC, indicando que eles estão em uma configuração de MetroCluster Stretch ou conectado à malha.

Componentes	Cluster_A no site_A	Cluster_B no local_B
DR_Group_1-FC	• Node_A_1-FC • shelf_A_1 • shelf_A_2	• Nó_B_1-FC • shelf_B_1 • shelf_B_2
DR_Group_2-IP	• Node_A_1-IP • Node_A_2-IP • shelf_A_1 • shelf_A_2 • Shelf_A_3-novo • Shelf_A_4-novo	• Node_B_1-IP • Node_B_2-IP • shelf_B_1 • shelf_B_2 • Shelf_B_3-new • Shelf_B_4-new
Interrutores	• Switch_A_1-FC • Switch_A_2-FC • Switch_A_1-IP • Switch_A_2-IP	• Switch_B_1-FC • Switch_B_2-FC • Switch_B_1-IP • Switch_B_2-IP

Preparação para uma transição disruptiva de FC para IP

Antes de iniciar o processo de transição, você deve garantir que a configuração atenda aos requisitos.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a

criação de casos durante a atividade de manutenção.

Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Requisitos gerais para a transição FC para IP disruptiva

A configuração existente do MetroCluster FC deve atender aos seguintes requisitos:

- Ela precisa ser uma configuração de dois nós e todos os nós precisam estar executando o ONTAP 9.8 ou posterior.

  Pode ser um MetroCluster com dois nós conectados a malha ou estendido.

- Ele deve atender a todos os requisitos e cabeamento, conforme descrito nos procedimentos *Instalação e Configuração do MetroCluster*.

  "Instalação e configuração do MetroCluster conectado à malha"

  "Instalação e configuração do Stretch MetroCluster"

- Ele não pode ser configurado com criptografia de armazenamento NetApp (NSE).
- Os volumes MDV não podem ser encriptados.

Você precisa ter acesso remoto ao console para todos os seis nós do site MetroCluster ou Planejar a viagem entre os locais conforme necessário pelo procedimento.

Reutilização do compartimento de unidade e requisitos de unidade para uma transição FC para IP disruptiva

Você precisa garantir que as unidades sobressalentes e o espaço agregado de raiz adequados estejam disponíveis nas gavetas de storage.

Reutilização das gavetas de storage existentes

Ao usar esse procedimento, as prateleiras de armazenamento existentes são mantidas para uso pela nova configuração. Quando node_A_1-FC e node_B_1-FC são removidos, as prateleiras de unidades existentes são conetadas ao node_A_1-IP e node_A_2-IP no cluster_A e node_B_1-IP e node_B_2-IP no cluster_B.

- Os novos modelos de plataforma devem oferecer suporte aos novos modelos de plataforma para os compartimentos de storage existentes (aqueles conectados a node_A_1-FC e node_B_1-FC).

  Se as gavetas existentes não forem compatíveis com os novos modelos de plataforma, "Transição sem interrupções quando as gavetas atuais não são compatíveis com novos controladores (ONTAP 9.8 e posterior)"consulte .

- Você deve garantir que não exceda os limites da plataforma para unidades, etc.

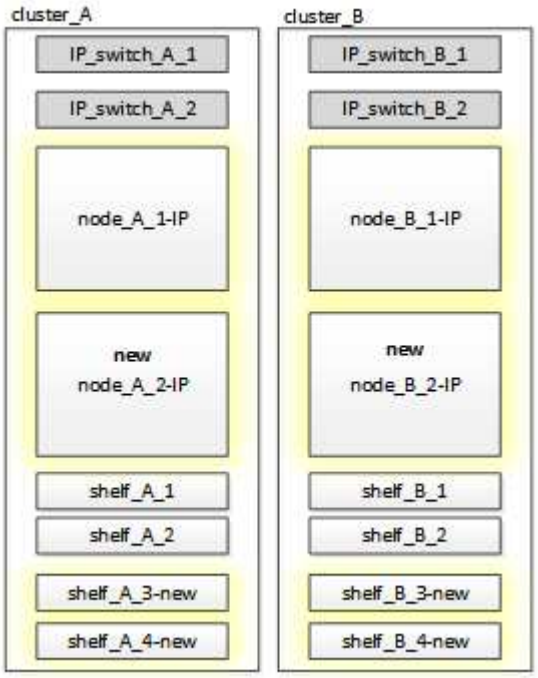
  "NetApp Hardware Universe"

Requisitos de storage para controladores adicionais

Armazenamento adicional deve ser adicionado, se necessário, para acomodar os dois controladores adicionais (node_A_2-IP e node_B_2-ip), porque a configuração está mudando de um arranjo de dois nós para um de quatro nós.

- Dependendo das unidades sobressalentes disponíveis nas gavetas existentes, é necessário adicionar unidades adicionais para acomodar controladores adicionais na configuração.

  Isso pode exigir prateleiras de armazenamento adicionais, como mostrado na ilustração a seguir.



  Você precisa ter mais 14 a 18 unidades cada para o terceiro e quarto controladores (node_A_2-IP e node_B_2-IP):

  - Três unidades de pool0 TB
  - Três unidades de pool1 TB
  - Duas unidades de reserva
  - Seis a dez unidades para o volume do sistema
- Você deve garantir que a configuração, incluindo os novos nós, não exceda os limites da plataforma para a configuração, incluindo contagem de unidades, capacidade de tamanho de agregado raiz, etc.

  Esta informação está disponível para cada modelo de plataforma em *NetApp Hardware Universe*.

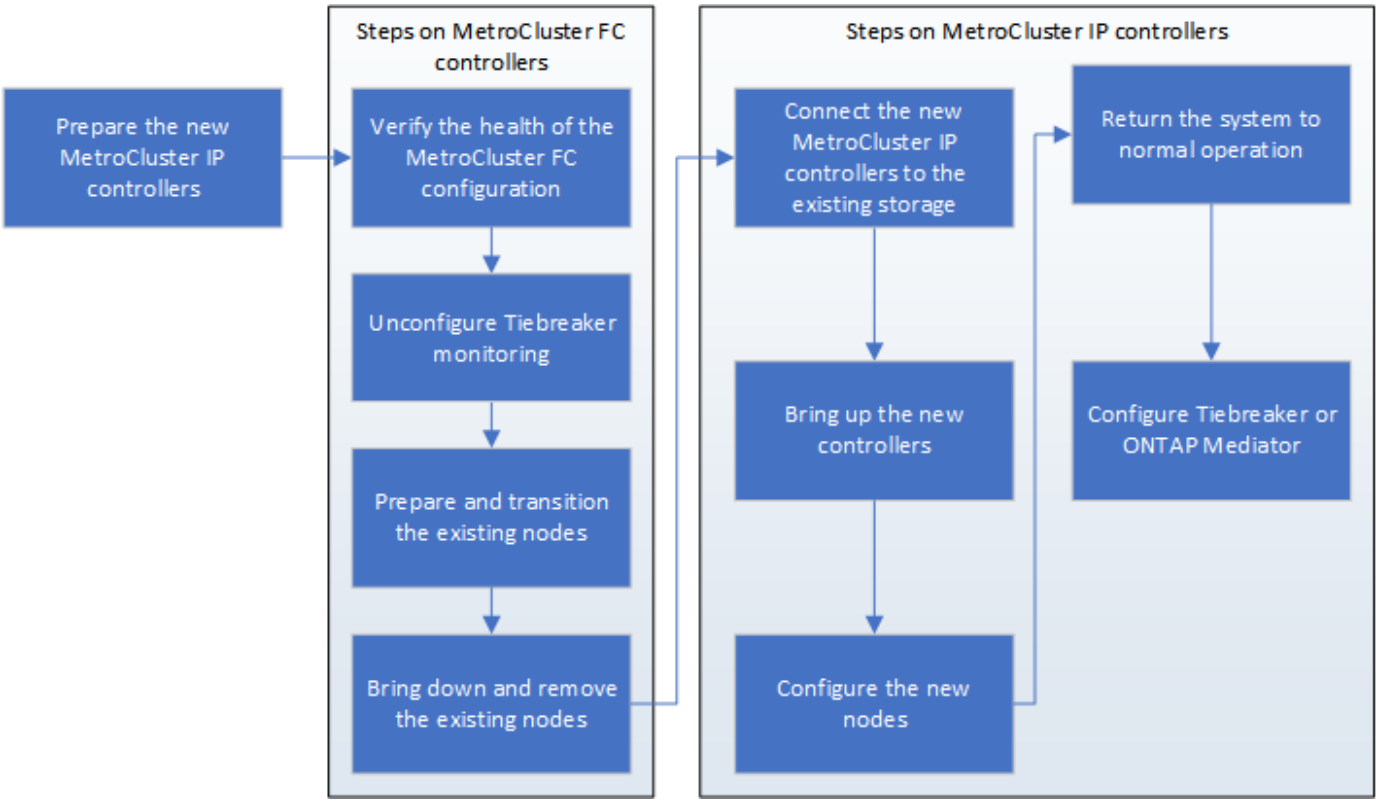
  "NetApp Hardware Universe"

Fluxo de trabalho para transição disruptiva

Você deve seguir o fluxo de trabalho específico para garantir uma transição bem-sucedida.

Enquanto você se prepara para a transição, Planeje viagens entre os sites. Observe que depois que os nós remotos forem colocados em rack e cabeados, você precisará ter acesso ao terminal serial aos nós. O acesso

ao processador de serviço não estará disponível até que os nós sejam configurados.



Mapeamento de portas dos nós FC do MetroCluster para os nós IP do MetroCluster

Você precisa ajustar a configuração de porta e LIF do nó MetroCluster FC para que seja compatível com a do nó IP MetroCluster que o substituirá.

Sobre esta tarefa

Quando os novos nós são inicializados pela primeira vez durante o processo de atualização, cada nó usa a configuração mais recente do nó que está substituindo. Quando você inicializa node_A_1-IP, o ONTAP tenta hospedar LIFs nas mesmas portas que foram usadas no node_A_1-FC.

Durante o procedimento de transição, você executará etapas nos nós antigos e novos para garantir a configuração correta de cluster, gerenciamento e LIF de dados.

Passos

1. Identifique quaisquer conflitos entre o uso da porta FC MetroCluster existente e o uso da porta para as interfaces IP do MetroCluster nos novos nós.

   Você deve identificar as portas IP do MetroCluster nos novos controladores IP do MetroCluster usando a tabela abaixo. Em seguida, verifique e Registre se existem LIFs de dados ou LIFs de cluster nessas portas nos nós FC do MetroCluster.

   Esses LIFs de dados conflitantes ou LIFs de cluster nos nós FC do MetroCluster serão movidos na etapa apropriada no procedimento de transição.

   A tabela a seguir mostra as portas IP MetroCluster por modelo de plataforma. Você pode ignorar a coluna VLAN ID.

Modelo de plataforma	Porta IP MetroCluster	ID DA VLAN	

AFF A800	e0b	Não utilizado	
	e1b		
AFF A700 e FAS9000	e5a		
	e5b		
AFF A320	e0g		
	e0h		
AFF A300 e FAS8200	e1a		
	e1b		
FAS8300/A400/FAS8700	e1a	10	
	e1b	20	
AFF A250 e FAS500f	e0c	10	
	e0b	20	

Você pode preencher a tabela a seguir e consultá-la posteriormente no procedimento de transição.

Portas	Portas de interface IP MetroCluster correspondentes (da tabela acima)	LIFs conflitantes nessas portas nos nós FC do MetroCluster
Primeira porta IP MetroCluster em node_A_1-FC		
Segunda porta IP MetroCluster em node_A_1-FC		
Primeira porta IP MetroCluster em node_B_1-FC		
Segunda porta IP MetroCluster no node_B_1-FC		

2. Determine quais portas físicas estão disponíveis nos novos controladores e quais LIFs podem ser hospedados nas portas.

   O uso da porta do controlador depende do modelo da plataforma e do modelo do switch IP que você usará na configuração IP do MetroCluster. Você pode coletar o uso de portas das novas plataformas a partir do

NetApp Hardware Universe.

"NetApp Hardware Universe"

3. Se desejar, Registre as informações da porta para node_A_1-FC e node_A_1-IP.

   Irá consultar a tabela à medida que realizar o procedimento de transição.

   Nas colunas node_A_1-IP, adicione as portas físicas para o novo módulo de controlador e Planeje os domínios IPspaces e broadcast para o novo nó.

	Node_A_1-FC			Node_A_1-IP		
LIF	Portas	IPspaces	Domínios de broadcast	Portas	IPspaces	Domínios de broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gerenciamento de nós						
Gerenciamento de clusters						
Dados 1						
Dados 2						
Dados 3						
Dados 4						
SAN						
Porta entre clusters						

4. Se desejar, Registre todas as informações de porta para node_B_1-FC.

   Irá consultar a tabela à medida que realizar o procedimento de atualização.

   Nas colunas de node_B_1-IP, adicione as portas físicas para o novo módulo de controlador e Planeje o uso da porta LIF, IPspaces e domínios de broadcast para o novo nó.

	Nó_B_1-FC			Node_B_1-IP		
LIF	Portas físicas	IPspaces	Domínios de broadcast	Portas físicas	IPspaces	Domínios de broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gerenciamento de nós						
Gerenciamento de clusters						
Dados 1						
Dados 2						
Dados 3						
Dados 4						
SAN						
Porta entre clusters						

Preparação dos controladores IP MetroCluster

Você deve preparar os quatro novos nós IP do MetroCluster e instalar a versão correta do ONTAP.

Sobre esta tarefa

Esta tarefa deve ser executada em cada um dos novos nós:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

Os nós devem ser conetados a qualquer **new** storage shelves. Eles devem **não** ser conetados às prateleiras de armazenamento existentes que contêm dados.

Essas etapas podem ser executadas agora ou mais tarde no procedimento quando os controladores e as

gavetas forem desmontados. Em qualquer caso, você deve limpar a configuração e preparar os nós **antes** conetando-os às prateleiras de storage existentes e **antes** fazer alterações de configuração nos nós FC do MetroCluster.

> Não execute estas etapas com os controladores MetroCluster IP conectados aos compartimentos de storage existentes que foram conectados aos controladores MetroCluster FC.

Nestas etapas, você limpa a configuração nos nós e limpa a região da caixa de correio em novas unidades.

Passos

1. Conete os módulos de controladora às novas gavetas de storage.
2. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   ```
   ha-config show
   ```

   O estado HA para todos os componentes deve ser "mccip".

3. Se o estado do sistema apresentado do controlador ou do chassis não estiver correto, defina o estado HA:

   ```
   ha-config modify controller mccip``ha-config modify chassis mccip
   ```

4. Sair do modo de manutenção:

   ```
   halt
   ```

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

5. Repita as seguintes subetapas em todos os quatro nós para limpar a configuração:

   a. Defina as variáveis ambientais como valores padrão:

      ```
      set-defaults
      ```

   b. Salvar o ambiente:

      ```
      saveenv
      ```

   ```
   bye
   ```

6. Repita as seguintes subetapas para inicializar todos os quatro nós usando a opção 9a no menu de inicialização.

   a. No prompt DO Loader, inicie o menu de inicialização:

      ```
      boot_ontap menu
      ```

   b. No menu de inicialização, selecione a opção ""9a"" para reinicializar o controlador.

7. Inicialize cada um dos quatro nós para o modo Manutenção usando a opção "'5" no menu de inicialização.
8. Registre a ID do sistema e de cada um dos quatro nós:

   ```
   sysconfig
   ```

9. Repita as etapas a seguir em node_A_1-IP e node_B_1-IP.
    a. Atribua a propriedade de todos os discos locais a cada site:

       ```
       disk assign adapter.xx.*
       ```

    b. Repita a etapa anterior para cada HBA com compartimentos de unidades anexados no node_A_1-IP e node_B_1-IP.
10. Repita as etapas a seguir em node_A_1-IP e node_B_1-IP para limpar a região da caixa de correio em cada disco local.
    a. Destrua a região da caixa de correio em cada disco:

       ```
       mailbox destroy local``mailbox destroy partner
       ```

11. Parar todas as quatro controladoras:

    ```
    halt
    ```

12. Em cada controlador, exiba o menu de inicialização:

    ```
    boot_ontap menu
    ```

13. Em cada um dos quatro controladores, limpe a configuração:

    ```
    wipeconfig
    ```

    Quando a operação wipeconfig for concluída, o nó retorna automaticamente ao menu de inicialização.

14. Repita as seguintes subetapas para inicializar novamente todos os quatro nós usando a opção 9a no menu de inicialização.
    a. No prompt DO Loader, inicie o menu de inicialização:

       ```
       boot_ontap menu
       ```

    b. No menu de inicialização, selecione a opção ""9a"" para reinicializar o controlador.
    c. Deixe o módulo controlador concluir a inicialização antes de passar para o próximo módulo controlador.

    Depois que "'9a" é concluído, os nós retornam automaticamente ao menu de inicialização.

15. Desligue os controladores.

Verificando a integridade da configuração do MetroCluster FC

Você deve verificar a integridade e a conectividade da configuração do MetroCluster FC antes de realizar a transição

Esta tarefa é executada na configuração MetroCluster FC.

1. Verifique a operação da configuração do MetroCluster no ONTAP:
    a. Verifique se o sistema é multipathed:

       ```
       node run -node node-name sysconfig -a
       ```

b. Verifique se há alertas de integridade em ambos os clusters:

```
system health alert show
```

c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

```
metrocluster show
```

d. Execute uma verificação MetroCluster:

```
metrocluster check run
```

e. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

f. Verifique se existem alertas de estado nos interrutores (se presentes):

```
storage switch show
```

g. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

h. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

2. Verifique se os nós estão no modo não HA:

```
storage failover show
```

Remoção da configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes da transição.

Passos

1. Remova a configuração existente do MetroCluster do software tiebreaker.

"Remoção das configurações do MetroCluster"

2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

Consulte a documentação da aplicação.

Fazendo a transição dos nós do MetroCluster FC

Você precisa coletar informações dos nós FC do MetroCluster existentes, enviar uma mensagem do AutoSupport anunciando o início da manutenção e fazer a transição dos nós.

Recolha de informações dos módulos do controlador existentes antes da transição

Antes da transição, você deve reunir informações para cada um dos nós.

Esta tarefa é executada nos nós existentes:

- Node_A_1-FC
- Nó_B_1-FC

a. Reúna a saída para os comandos na tabela a seguir.

Categoria	Comandos	Notas
Licença	show de licença do sistema	
Compartimentos e números de discos em cada gaveta e detalhes de storage flash, memória e NVRAM e placas de rede	o nó do sistema executa -node node_name sysconfig	
LIFs de gerenciamento de nós e rede de cluster	o nó do sistema executa -node_name sysconfig interface de rede show -role "cluster,node-mgmt,data"	
Informações sobre SVM	mostra o svm	
Informações do protocolo	show de nfs show iscsi show cifs	
Portas físicas	network port show -node node_name -type physical network port show	
Grupos de failover	os grupos de failover de interface de rede mostram -vserver vserver_name	Registre os nomes e as portas dos grupos de failover que não estão em toda a extensão.
Configuração VLAN	vlan show -node node_name	Registre cada porta de rede e emparelhamento de ID VLAN.
Configuração do grupo de interfaces	porta de rede ifgrp show -node node_name -instance	Registre os nomes dos grupos de interface e as portas atribuídas a eles.
Domínios de broadcast	exibição de domínio de broadcast da porta de rede	
IPspace	show do ipspace da rede	
Informações de volume	mostra de volume e mostra de volume -campos encriptados	
Informações agregadas	exibição de agregados de armazenamento e armazenamento de dados de criptografia aggr show eshow de armazenamento de objetos agregados de armazenamento de armazenamento de dados	

Categoria	Comandos	Notas
Informações de propriedade do disco	exibição de agregados de armazenamento e armazenamento de dados de criptografia aggr show eshow de armazenamento de objetos agregados de armazenamento de armazenamento de dados	
Criptografia	exibição de caixa de correio-disco de failover de armazenamento e backup de gerenciador de chaves de segurança show	Preservar também a frase-passe utilizada para ativar o gestor de chaves. No caso do gerenciador de chaves externo, você precisará das informações de autenticação para o cliente e servidor.
Criptografia	mostra o gerenciador de chaves de segurança	
Criptografia	show externo do gerenciador de chaves de segurança	
Criptografia	systemshell local kenv kmip.init.ipaddr endereço ip	
Criptografia	systemshell local kenv kmip.init.netmask netmask	
Criptografia	systemshell local kenv kmip.init.gateway gateway	
Criptografia	systemshell local kenv kmip.init.interface interface	

Enviar uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Isso impede que eles abram um caso partindo do pressuposto de que ocorreu uma interrupção.

Esta tarefa deve ser executada em cada site do MetroCluster.

1. Para evitar a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a manutenção está em andamento.
   a. Emita o seguinte comando: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      maintenance-window-in-hours especifica a duração da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repita o comando no cluster de parceiros.

Fazer a transição, encerrar e remover os nós do MetroCluster FC

Além de emitir comandos nos nós FC do MetroCluster, essa tarefa inclui o cabeamento físico e a remoção dos módulos da controladora em cada local.

Esta tarefa deve ser executada em cada um dos nós antigos:

- Node_A_1-FC
- Nó_B_1-FC

Passos

1. Parar todo o tráfego do cliente.
2. Em qualquer um dos nós FC do MetroCluster, por exemplo, node_A_1-FC, habilite a transição.
   a. Defina o nível de privilégio avançado: `set -priv advanced`
   b. Ativar transição: `metrocluster transition enable -transition-mode disruptive`
   c. Voltar ao modo de administração: `set -priv admin`
3. Desespelhar o agregado de raiz excluindo o Plex remoto dos agregados de raiz.
   a. Identificar os agregados de raiz: `storage aggregate show -root true`
   b. Exibir os pool1 agregados: `storage aggregate plex show -pool 1`
   c. Off-line e excluir o Plex remoto do agregado raiz
   `aggr plex offline <root-aggregate> -plex <remote-plex-for-root-aggregate>`

   `aggr plex delete <root-aggregate> -plex <remote-plex-for-root-aggregate>`

   Por exemplo:

```
# aggr plex offline aggr0_node_A_1-FC_01 -plex remoteplex4
```

+

```
# aggr plex delete aggr0_node_A_1-FC_01 -plex remoteplex4
```

4. Confirme a contagem da caixa de correio, atribuição automática do disco e modo de transição antes de continuar usando os seguintes comandos em cada controlador:
   a. Defina o nível de privilégio avançado: `set -priv advanced`
   b. Confirme se apenas três unidades de caixa de correio são mostradas para cada módulo do controlador: `storage failover mailbox-disk show`
   c. Voltar ao modo de administração: `set -priv admin`
   d. Confirme se o modo de transição é disruptivo: MetroCluster Transition show
5. Verifique se há discos quebrados: `disk show -broken`
6. Remova ou substitua quaisquer discos quebrados

7. Confirme se os agregados estão íntegros usando os seguintes comandos em node_A_1-FC e node_B_1-FC:

   ```
   storage aggregate show

   storage aggregate plex show
   ```

   O comando storage Aggregate show indica que o agregado raiz é sem espelhamento.

8. Verifique se há VLANs ou grupos de interface:

   ```
   network port ifgrp show

   network port vlan show
   ```

   Se nenhuma estiver presente, ignore as duas etapas a seguir.

9. Exiba a lista de LIfs usando VLANs ou ifgrps:

   ```
   network interface show -fields home-port,curr-port

   network port show -type if-group | vlan
   ```

10. Remova quaisquer VLANs e grupos de interface.

    Você deve executar essas etapas para todos os LIFs em todos os SVMs, incluindo aqueles SVMs com o sufixo -mc.

    a. Mova quaisquer LIFs usando as VLANs ou grupos de interface para uma porta disponível: `network interface modify -vserver vserver-name -lif lif_name -home- port port`
    b. Exiba os LIFs que não estão em suas portas iniciais: `network interface show -is-home false`
    c. Reverter todos os LIFs para suas respetivas portas residenciais: `network interface revert -vserver vserver_name -lif lif_name`
    d. Verifique se todos os LIFs estão em suas portas residenciais: `network interface show -is -home false`

       Não devem aparecer LIFs na saída.

    e. Remova as portas VLAN e ifgrp do domínio de broadcast: `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`
    f. Verifique se todas as portas vlan e ifgrp não estão atribuídas a um domínio de broadcast: `network port show -type if-group | vlan`
    g. Eliminar todas as VLANs: `network port vlan delete -node nodename -vlan-name vlan-name`
    h. Eliminar grupos de interface: `network port ifgrp delete -node nodename -ifgrp ifgrp-name`

11. Mova quaisquer LIFs conforme necessário para resolver conflitos com as portas de interface IP do MetroCluster.

É necessário mover os LIFs identificados na etapa 1 do "Mapeamento de portas dos nós FC do MetroCluster para os nós IP do MetroCluster".

a. Mova quaisquer LIFs hospedados na porta desejada para outra porta: `network interface modify -lif lifname -vserver vserver-name -home-port new-homeport``network interface revert -lif lifname -vserver vservername`

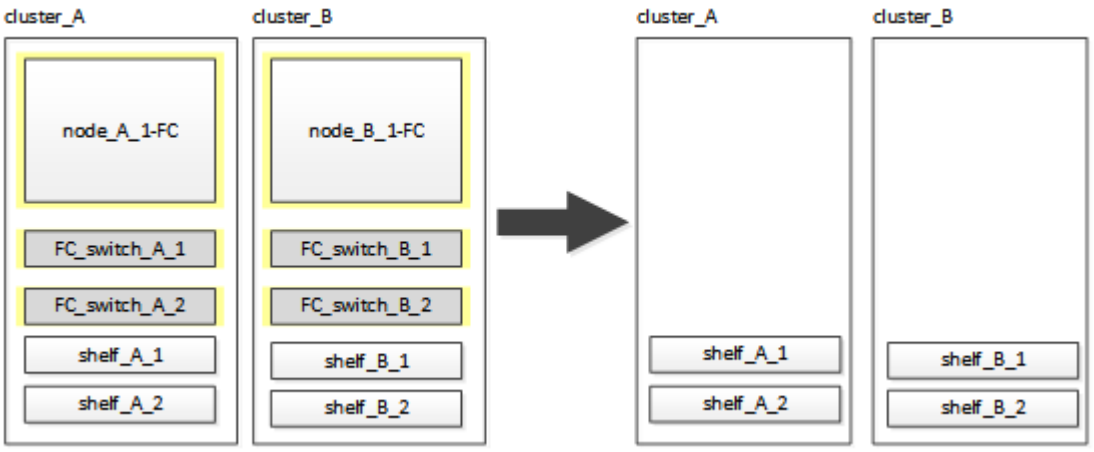
b. Se necessário, mova a porta de destino para um domínio IPspace e broadcast apropriado. `network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast -domain current-broadcast-domain -ports controller-name:current-port``network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port`

12. Parar os controladores MetroCluster FC (node_A_1-FC e node_B_1-FC): `system node halt`
13. No prompt Loader, sincronize os relógios de hardware entre os módulos do controlador FC e IP.
    a. No nó FC MetroCluster antigo (node_A_1-FC), exiba a data: `show date`
    b. Nos novos controladores IP MetroCluster (node_A_1-IP e node_B_1-IP), defina a data mostrada no controlador original: `set date mm/dd/yy`
    c. Nos novos controladores IP MetroCluster (node_A_1-IP e node_B_1-IP), verifique a data: `show date`
14. Parar e desligar os módulos de controladora FC MetroCluster (node_A_1-FC e node_B_1-FC), pontes FC para SAS (se presentes), switches FC (se presentes) e cada compartimento de storage conectado a esses nós.
15. Desconete as gavetas dos controladores FC MetroCluster e documente quais gavetas são storage local para cada cluster.

    Se a configuração usar bridges FC para SAS ou switches de back-end FC, desconete-os e remova-os.

16. No modo Manutenção nos nós FC do MetroCluster (node_A_1-FC e node_B_1-FC), confirme se não há discos conetados: `disk show -v`
17. Desligue e remova os nós de FC do MetroCluster.

Nesse ponto, as controladoras MetroCluster FC foram removidas e as gavetas foram desconetadas de todas as controladoras.



Ligar os módulos do controlador IP MetroCluster

É necessário adicionar os quatro novos módulos de controladora e quaisquer compartimentos de storage adicionais à configuração. Os novos módulos do controlador são adicionados dois-por-vez.

Configurando os novos controladores

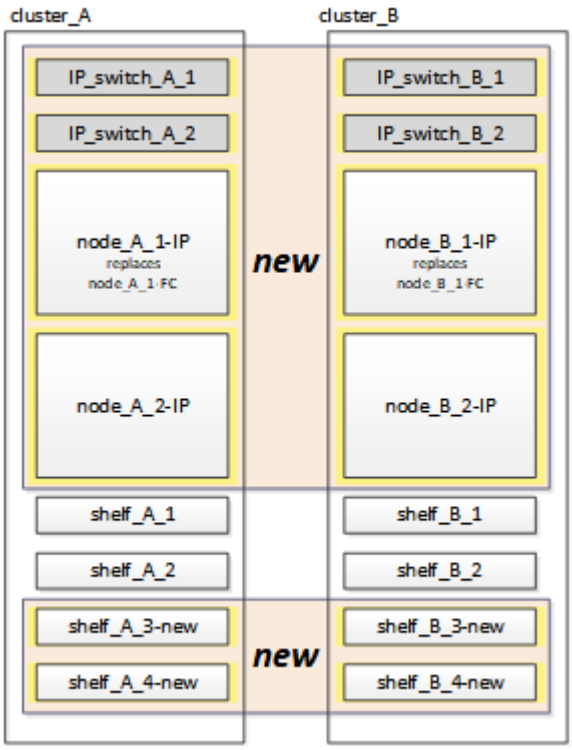
É necessário colocar em rack e cabo as novas controladoras MetroCluster IP até as gavetas de storage conectadas anteriormente às controladoras MetroCluster FC.

Sobre esta tarefa

Essas etapas devem ser executadas em cada um dos nós IP do MetroCluster.

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

No exemplo a seguir, duas gavetas de storage adicionais são adicionadas em cada local para fornecer storage para acomodar os novos módulos de controladora.



Passos

1. Planeje o posicionamento dos novos módulos de controladora e compartimentos de armazenamento conforme necessário.

   O espaço em rack depende do modelo de plataforma dos módulos de controladora, dos tipos de switch e do número de compartimentos de storage em sua configuração.

2. Aterre-se corretamente.
3. Montar o novo equipamento em rack: Controladores, compartimentos de storage e switches IP.

   Não faça cabos nas prateleiras de armazenamento ou nos switches IP neste momento.

4. Conete os cabos de alimentação e a conexão do console de gerenciamento aos controladores.
5. Verifique se todas as prateleiras de armazenamento estão desligadas.
6. Verifique se nenhuma unidade está conetada executando as etapas a seguir em todos os quatro nós:

   a. No prompt DO Loader, inicie o menu de inicialização:

      ```
      boot_ontap maint
      ```

   b. Verifique se nenhuma unidade está conetada:

      ```
      disk show -v
      ```

   A saída não deve mostrar nenhuma unidade.

   a. Parar o nó:

      ```
      halt
      ```

7. Inicialize todos os quatro nós usando a opção 9a no menu de inicialização.

   a. No prompt DO Loader, inicie o menu de inicialização:

      ```
      boot_ontap menu
      ```

   b. No menu de inicialização, selecione a opção ""9a"" para reinicializar o controlador.
   c. Deixe o módulo controlador concluir a inicialização antes de passar para o próximo módulo controlador.

   Depois que "'9a" é concluído, os nós retornam automaticamente ao menu de inicialização.

8. Cable as prateleiras de armazenamento.

   Consulte os procedimentos de instalação e configuração da controladora para obter informações sobre o seu modelo.

   "Documentação dos sistemas de hardware da ONTAP"

9. Faça o cabeamento dos controladores para os switches IP, conforme descrito em "Cabeamento dos switches IP".
10. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

    Siga as etapas para o fornecedor do switch:

    - "Redefinindo o switch IP Broadcom para os padrões de fábrica"
    - "Repor as predefinições de fábrica do interrutor IP do Cisco"

11. Baixe e instale os arquivos RCF.

Siga as etapas para o fornecedor do switch:

- "Download e instalação dos arquivos RCF Broadcom"
- "Transferir e instalar os ficheiros Cisco IP RCF"

12. Ligue a energia para o primeiro novo controlador (node_A_1-IP) e pressione Ctrl-C para interromper o processo de inicialização e exibir o prompt Loader.
13. Inicialize o controlador para o modo de manutenção:

```
boot_ontap_maint
```

14. Apresentar a ID do sistema para o controlador:

```
sysconfig -v
```

15. Confirme se as gavetas da configuração existente estão visíveis a partir do novo nó IP do MetroCluster:

```
storage show shelf``disk show -v
```

16. Parar o nó:

```
halt
```

17. Repita as etapas anteriores no outro nó no site do parceiro (site_B).

Conexão e inicialização node_A_1-IP e node_B_1-IP

Depois de conetar os controladores IP do MetroCluster e os switches IP, você faz a transição e inicializa node_A_1-IP e node_B_1-IP.

Exibindo node_A_1-IP

Você deve inicializar o nó com a opção de transição correta.

Passos

1. Boot node_A_1-IP para o menu de inicialização:

```
boot_ontap menu
```

2. Execute o seguinte comando no prompt do menu de inicialização para iniciar a transição:

```
boot_after_mcc_transition
```

   - Esse comando reatribui todos os discos de propriedade de node_A_1-FC ao node_A_1-IP.
     - Os discos Node_A_1-FC são atribuídos a node_A_1-IP
     - Os discos Node_B_1-FC são atribuídos ao node_B_1-IP
   - O comando também faz automaticamente outras reatribuições de ID do sistema necessárias para que os nós IP do MetroCluster possam ser inicializados no prompt do ONTAP.
   - Se o comando boot_after_mcc_transition falhar por qualquer motivo, ele deve ser executado novamente a partir do menu de inicialização.

- Se o seguinte prompt for exibido, digite Ctrl-C para continuar. A verificar o estado do recetáculo de diagnóstico MCC… [Enter Ctrl-C(resume), S(status), L(link)]_
- Se o volume raiz foi criptografado, o nó será interrompido com a seguinte mensagem. Parar o sistema, porque o volume raiz está encriptado (encriptação de volume NetApp) e a importação de chaves falhou. Se esse cluster estiver configurado com gerenciador de chaves externo (KMIP), verifique a integridade dos servidores de chaves.

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning. Selection (1-9)?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-
FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of
MetroCluster FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
```

3. Se os volumes de dados estiverem criptografados, restaure as chaves usando o comando correto para a configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gestão de chaves a bordo	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .

Gerenciamento de chaves externas	`security key-manager key query -node node-name` Para obter mais informações, "Restaurar chaves de criptografia de gerenciamento de chaves externas"consulte .

4. Se o volume raiz estiver encriptado, utilize o procedimento em "Recuperar o gerenciamento de chaves se o volume raiz for criptografado".

Recuperar o gerenciamento de chaves se o volume raiz for criptografado

Se o volume raiz estiver criptografado, você deve usar comandos especiais de inicialização para restaurar o gerenciamento de chaves.

Antes de começar

Você deve ter as senhas reunidas mais cedo.

Passos

1. Se o gerenciamento de chaves integradas for usado, execute as seguintes etapas para restaurar a configuração.

   a. No prompt Loader, exiba o menu de inicialização:

      `boot_ontap menu`

   b. Selecione a opção ""(10) Definir segredos de recuperação de gerenciamento de chaves integradas" no menu de inicialização.

      Responda conforme apropriado aos prompts:

      ```
      This option must be used only in disaster recovery procedures. Are
      you sure? (y or n): y
      Enter the passphrase for onboard key management: passphrase
      Enter the passphrase again to confirm: passphrase

      Enter the backup data: backup-key
      ```

      O sistema arranca para o menu de arranque.

   c. Insira a opção "'6" no menu de inicialização.

      Responda conforme apropriado aos prompts:

```
This will replace all flash-based configuration with the last backup
to
disks. Are you sure you want to continue?: y

Following this, the system will reboot a few times and the following
prompt will be available continue by saying y

WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
```

Após a reinicialização, o sistema estará no prompt DO Loader.

d. No prompt Loader, exiba o menu de inicialização:

```
boot_ontap menu
```

e. Novamente, selecione a opção ""(10) Definir segredos de recuperação de gerenciamento de chaves integradas" no menu de inicialização.

Responda conforme apropriado aos prompts:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

O sistema arranca para o menu de arranque.

f. Insira a opção "'1" no menu de inicialização.

Se o seguinte prompt for exibido, você pode pressionar Ctrl para retomar o processo.

```
 Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
```

O sistema inicia no prompt ONTAP.

g. Restaure o gerenciamento de chaves integradas:

```
security key-manager onboard sync
```

Responda conforme apropriado aos prompts, usando a senha que você coletou anteriormente:

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster_A":: passphrase
```

2. Se o gerenciamento de chaves externas for usado, execute as seguintes etapas para restaurar a configuração.

   a. Defina os bootargs necessários:

      ```
      setenv bootarg.kmip.init.ipaddr ip-address

      setenv bootarg.kmip.init.netmask netmask

      setenv bootarg.kmip.init.gateway gateway-address

      setenv bootarg.kmip.init.interface interface-id
      ```

   b. No prompt Loader, exiba o menu de inicialização:

      ```
      boot_ontap menu
      ```

   c. Selecione a opção ""(11) Configure node for external key Management" no menu de inicialização.

      O sistema arranca para o menu de arranque.

   d. Insira a opção "'6" no menu de inicialização.

      O sistema arranca várias vezes. Você pode responder afirmativamente quando solicitado a continuar o processo de inicialização.

      Após a reinicialização, o sistema estará no prompt DO Loader.

   e. Defina os bootargs necessários:

      ```
      setenv bootarg.kmip.init.ipaddr ip-address

      setenv bootarg.kmip.init.netmask netmask

      setenv bootarg.kmip.init.gateway gateway-address
      ```

```
setenv bootarg.kmip.init.interface interface-id
```

   a. No prompt Loader, exiba o menu de inicialização:

      ```
      boot_ontap menu
      ```

   b. Selecione novamente a opção "'(11) Configure node for external key Management" no menu de inicialização e responda às solicitações conforme necessário.

      O sistema arranca para o menu de arranque.

   c. Restaure o gerenciamento de chaves externas:

```
security key-manager external restore
```

Criando a configuração de rede

Você deve criar uma configuração de rede que corresponda à configuração nos nós FC. Isso ocorre porque o nó IP do MetroCluster replays a mesma configuração quando ele é inicializado, o que significa que, quando node_A_1-IP e node_B_1-IP iniciarem, o ONTAP tentará hospedar LIFs nas mesmas portas que foram usadas em node_A_1-FC e node_B_1-FC respetivamente.

Sobre esta tarefa

À medida que cria a configuração de rede, utilize o plano apresentado "Mapeamento de portas dos nós FC do MetroCluster para os nós IP do MetroCluster"para o ajudar.

Configuração adicional pode ser necessária para abrir LIFs de dados depois que os nós IP do MetroCluster tiverem sido configurados.

Passos

1. Verifique se todas as portas de cluster estão no domínio de broadcast apropriado:

   O IPspace do cluster e o domínio de broadcast do cluster são necessários para criar LIFs de cluster

   a. Visualizar os espaços IP:

      ```
      network ipspace show
      ```

   b. Crie espaços IP e atribua portas de cluster conforme necessário.

      "Configurando IPspaces (somente administradores de cluster)"

   c. Veja os domínios de broadcast:

      ```
      network port broadcast-domain show
      ```

   d. Adicione todas as portas de cluster a um domínio de broadcast conforme necessário.

      "Adicionar ou remover portas de um domínio de broadcast"

   e. Recrie VLANs e grupos de interface conforme necessário.

      A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

      "Criando um VLAN"

   "Combinando portas físicas para criar grupos de interface"

2. Verifique se as configurações de MTU estão definidas corretamente para as portas e o domínio de broadcast e faça alterações usando os seguintes comandos:

   ```
   network port broadcast-domain show

   network port broadcast-domain modify -broadcast-domain bcastdomainname -mtu
   mtu-value
   ```

Configuração de portas de cluster e LIFs de cluster

Você deve configurar portas de cluster e LIFs. As etapas a seguir precisam ser executadas no site A nodos que foram inicializados com agregados de raiz.

Passos

1. Identifique a lista de LIFs usando a porta de cluster desejada:

   ```
   network interface show -curr-port portname

   network interface show -home-port portname
   ```

2. Para cada porta de cluster, altere a porta inicial de qualquer um dos LIFs nessa porta para outra porta,

   a. Entre no modo de privilégio avançado e digite "'y'" quando solicitado a continuar:

      ```
      set priv advanced
      ```

   b. Se o LIF que está sendo modificado é um LIF de dados:

      ```
      vserver config override -command "network interface modify -lif lifname
      -vserver vservername -home-port new-datahomeport"
      ```

   c. Se o LIF não for um LIF de dados:

      ```
      network interface modify -lif lifname -vserver vservername -home-port new-
      datahomeport
      ```

   d. Reverter os LIFs modificados para sua porta inicial:

      ```
      network interface revert * -vserver vserver_name
      ```

   e. Verifique se não há LIFs na porta do cluster:

      ```
      network interface show -curr-port portname
      ```

   ```
   network interface show -home-port portname
   ```

   a. Remova a porta do domínio de broadcast atual:

      ```
      network port broadcast-domain remove-ports -ipspace ipspacename -broadcast
      -domain bcastdomainname -ports node_name:port_name
      ```

   b. Adicione a porta ao domínio de IPspace e broadcast do cluster:

      ```
      network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain
      Cluster -ports node_name:port_name
      ```

   c. Verifique se a função da porta foi alterada: `network port show`

   d. Repita essas subetapas para cada porta de cluster.

   e. Voltar ao modo de administração:

      ```
      set priv admin
      ```

3. Crie LIFs de cluster nas novas portas de cluster:
   a. Para configuração automática usando endereço link local para cluster LIF, use o seguinte comando:

      ```
      network interface create -vserver Cluster -lif cluster_lifname -service
      -policy default-cluster -home-node a1name -home-port clusterport -auto true
      ```

   b. Para atribuir endereço IP estático para o cluster LIF, use o seguinte comando:

      ```
      network interface create -vserver Cluster -lif cluster_lifname -service
      -policy default-cluster -home-node a1name -home-port clusterport -address
      ip-address -netmask netmask -status-admin up
      ```

Verificando a configuração de LIF

O LIF de gerenciamento de nós, o LIF de gerenciamento de cluster e o LIF entre clusters ainda estarão presentes após o movimento de armazenamento do controlador antigo. Se necessário, você deve mover LIFs para portas apropriadas.

Passos

1. Verifique se o LIF de gerenciamento e as LIFs de gerenciamento de cluster já estão na porta desejada:

   ```
   network interface show -service-policy default-management

   network interface show -service-policy default-intercluster
   ```

   Se os LIFs estiverem nas portas desejadas, você poderá ignorar o restante dos passos nesta tarefa e prosseguir para a próxima tarefa.

2. Para cada nó, gerenciamento de cluster ou LIFs entre clusters que não estejam na porta desejada, altere a porta inicial de qualquer um dos LIFs nessa porta para outra porta.
   a. Reutilize a porta desejada movendo quaisquer LIFs hospedados na porta desejada para outra porta:

      ```
      vserver config override -command "network interface modify -lif lifname
      -vserver vservername -home-port new-datahomeport"
      ```

   b. Reverter os LIFs modificados para sua nova porta inicial:

      ```
      vserver config override -command "network interface revert -lif lifname
      -vserver _vservername"
      ```

   c. Se a porta desejada não estiver no domínio IPspace e broadcast correto, remova a porta do domínio IPspace e broadcast atual:

      ```
      network port broadcast-domain remove-ports -ipspace current-ipspace
      -broadcast-domain current-broadcast-domain -ports controller-name:current-
      port
      ```

   d. Mova a porta desejada para o domínio IPspace e broadcast correto:

      ```
      network port broadcast-domain add-ports -ipspace new-ipspace -broadcast
      -domain new-broadcast-domain -ports controller-name:new-port
      ```

e. Verifique se a função da porta foi alterada:

```
network port show
```

f. Repita essas subetapas para cada porta.

3. Mova o nó, LIFs de gerenciamento de cluster e LIF entre clusters para a porta desejada:

a. Alterar a porta inicial do LIF:

```
network interface modify -vserver vserver -lif node_mgmt -home-port port
-home-node homenode
```

b. Reverter o LIF para sua nova porta inicial:

```
network interface revert -lif node_mgmt -vserver vservername
```

c. Alterar a porta inicial do LIF de gerenciamento de cluster:

```
network interface modify -vserver vserver -lif cluster-mgmt-LIF-name -home
-port port -home-node homenode
```

d. Reverter o LIF de gerenciamento de cluster para sua nova porta inicial:

```
network interface revert -lif cluster-mgmt-LIF-name -vserver vservername
```

e. Alterar a porta inicial do LIF entre clusters:

```
network interface modify -vserver vserver -lif intercluster-lif-name -home
-node nodename -home-port port
```

f. Reverter o LIF entre clusters para sua nova porta inicial:

```
network interface revert -lif intercluster-lif-name -vserver vservername
```

Exibindo node_A_2-IP e node_B_2-IP

É necessário abrir e configurar o novo nó IP do MetroCluster em cada local, criando um par de HA em cada local.

Exibindo node_A_2-IP e node_B_2-IP

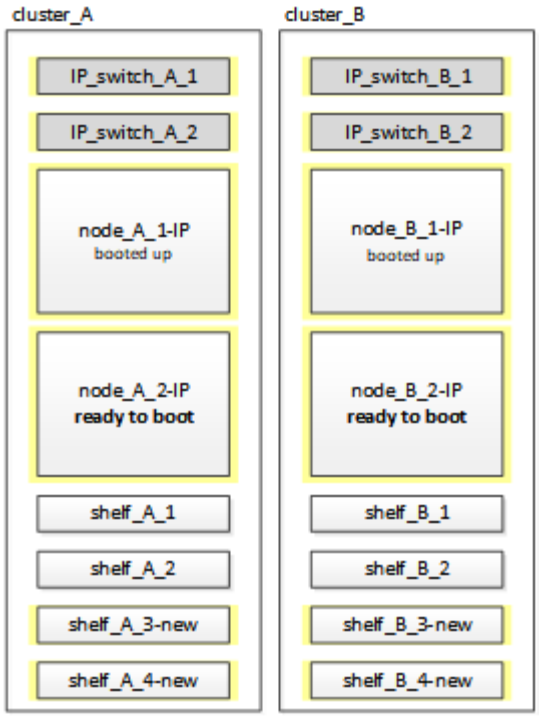
Você deve inicializar os novos módulos do controlador um de cada vez usando a opção correta no menu de inicialização.

Sobre esta tarefa

Nessas etapas, você inicializa os dois novos nós, expandindo o que havia sido uma configuração de dois nós em uma configuração de quatro nós.

Estas etapas são executadas nos seguintes nós:

- Node_A_2-IP
- Node_B_2-IP



Passos

1. Inicialize os novos nós usando a opção de inicialização "'9c".

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning. Selection (1-9)? 9c
```

O nó inicializa e inicia no assistente de configuração do nó, semelhante ao seguinte.

```
Welcome to node setup
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.
Any changes you made before quitting will be saved.
To accept a default or omit a question, do not enter a value. .
.
.
```

Se a opção "'9c" não for bem-sucedida, siga as seguintes etapas para evitar possíveis perdas de dados:

- Não tente executar a opção 9a.
- Desconete fisicamente as gavetas existentes que contêm dados da configuração original do MetroCluster FC (shelf_A_1, shelf_A_2, shelf_B_1, shelf_B_2).
- Entre em Contato com o suporte técnico, consultando o artigo da KB "Transição MetroCluster FC para IP - opção 9c com falha" .

  "Suporte à NetApp"

2. Ative a ferramenta AutoSupport seguindo as instruções fornecidas pelo assistente.
3. Responda aos prompts para configurar a interface de gerenciamento de nós.

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Verifique se o modo de failover de armazenamento está definido como HA:

   `storage failover show -fields mode`

   Se o modo não for HA, defina-o:

   `storage failover modify -mode ha -node` *`localhost`*

   Em seguida, você deve reiniciar o nó para que a alteração tenha efeito.

5. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

6. Saia do assistente de configuração do nó:

   ```
   exit
   ```

7. Faça login na conta de administrador usando o nome de usuário do administrador.
8. Junte-se ao cluster existente usando o assistente Configuração de cluster.

```
:> cluster setup
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and "exit"
or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

9. Depois de concluir o assistente de configuração do cluster e ele sair, verifique se o cluster está ativo e se o nó está em bom estado:

   ```
   cluster show
   ```

10. Desativar atribuição automática de disco:

    `storage disk option modify -autoassign off -node node_A_2-IP`

11. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gestão de chaves a bordo	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager key query -node` *`node-name`* Para obter mais informações, "Restaurar chaves de criptografia de gerenciamento de chaves externas"consulte .

12. Repita os passos acima no segundo novo módulo do controlador (node_B_2-IP).

Verificando as configurações da MTU

Verifique se as configurações de MTU estão definidas corretamente para as portas e o domínio de broadcast e faça alterações.

Passos

1. Verifique o tamanho da MTU usado no domínio de broadcast do cluster:

   `network port broadcast-domain show`

2. Se necessário, atualize o tamanho da MTU conforme necessário:

   `network port broadcast-domain modify -broadcast-domain` *`bcast-domain-name`* `-mtu` *`mtu-size`*

Configurando LIFs entre clusters

Configurar as LIFs entre clusters necessárias para peering de cluster.

Esta tarefa deve ser executada em ambos os novos nós, node_A_2-IP e node_B_2-IP.

Passo

1. Configurar as LIFs entre clusters. Consulte "Configurando LIFs entre clusters"

Verificando peering de cluster

Verifique se o cluster_A e o cluster_B são direcionados e os nós em cada cluster podem se comunicar uns com os outros.

Passos

1. Verifique a relação de peering de cluster:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
node_A_1-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
node_A_2-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

2. Ping para verificar se os endereços de pares estão acessíveis:

```
cluster peer ping -originating-node local-node -destination-cluster remote-cluster-name
```

Configurar os novos nós e concluir a transição

Com os novos nós adicionados, você deve concluir as etapas de transição e configurar os nós IP do MetroCluster.

Configurando os nós IP do MetroCluster e desativando a transição

Você deve implementar as conexões IP do MetroCluster, atualizar a configuração do MetroCluster e desativar o modo de transição.

Passos

1. Forme os novos nós em um grupo de DR emitindo os seguintes comandos do controller node_A_1-IP:

```
metrocluster configuration-settings dr-group create -partner-cluster
<peer_cluster_name> -local-node <local_controller_name> -remote-node
<remote_controller_name>

metrocluster configuration-settings dr-group show
```

2. Criar interfaces IP MetroCluster (node_A_1-IP, node_A_2-IP, node_B_1-IP, node_B_2-IP) - duas interfaces precisam ser criadas por controladora; oito interfaces no total:

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <controller_name> -home-port <port_name> -address
<ip_address> -netmask <netmask_address> -vlan-id <vlan_id>

metrocluster configuration-settings interface show
```

Certas plataformas usam uma VLAN para a interface IP do MetroCluster. Por padrão, cada uma das duas portas usa uma VLAN diferente: 10 e 20.

Se suportado, você também pode especificar uma VLAN diferente (não padrão) maior que 100 (entre 101 e 4095) usando o `-vlan-id` parâmetro no `metrocluster configuration-settings interface create` comando.

As seguintes plataformas **não** suportam o `-vlan-id` parâmetro:

- FAS8200 e AFF A300
- AFF A320
- FAS9000 e AFF A700
- AFF C800, ASA C800, AFF A800 e ASA A800

Todas as outras plataformas suportam o `-vlan-id` parâmetro.

As atribuições de VLAN padrão e válidas dependem se a plataforma suporta o `-vlan-id` parâmetro:

Plataformas que suportam <code>-vlan-id</code>

VLAN predefinida:

- Quando o `-vlan-id` parâmetro não é especificado, as interfaces são criadas com VLAN 10 para as portas "A" e VLAN 20 para as portas "B".
- A VLAN especificada deve corresponder à VLAN selecionada no RCF.

Intervalos de VLAN válidos:

- VLAN 10 e 20 padrão
- VLANs 101 e superior (entre 101 e 4095)

Plataformas que não suportam <code>-vlan-id</code>

VLAN predefinida:

- Não aplicável. A interface não requer que uma VLAN seja especificada na interface MetroCluster. A porta do switch define a VLAN que é usada.

Intervalos de VLAN válidos:

- Todas as VLANs não explicitamente excluídas ao gerar o RCF. O RCF alerta-o se a VLAN for inválida.

3. Execute a operação de conexão MetroCluster a partir do controlador node_A_1-IP para conetar os sites MetroCluster — esta operação pode levar alguns minutos para ser concluída:

```
metrocluster configuration-settings connection connect
```

4. Verifique se os discos de cluster remotos estão visíveis a partir de cada controlador através das ligações iSCSI:

   ```
   disk show
   ```

   Você deve ver os discos remotos pertencentes aos outros nós na configuração.

5. Espelhe o agregado de raiz para node_A_1-IP e node_B_1-IP:

   ```
   aggregate mirror -aggregate root-aggr
   ```

6. Atribua discos para node_A_2-IP e node_B_2-IP.

   Atribuições de disco do pool 1 onde já foram feitas para node_A_1-IP e node_B_1-IP quando o comando boot_after_mcc_transtion foi emitido no menu de inicialização.

   a. Emita os seguintes comandos no node_A_2-IP:

      ```
      disk assign disk1disk2disk3 … diskn -sysid node_B_2-IP-controller-sysid
      -pool 1 -force
      ```

   b. Emita os seguintes comandos no node_B_2-IP:

      ```
      disk assign disk1disk2disk3 … diskn -sysid node_A_2-IP-controller-sysid
      -pool 1 -force
      ```

7. Confirme que a propriedade foi atualizada para os discos remotos:

   ```
   disk show
   ```

8. Se necessário, atualize as informações de propriedade usando os seguintes comandos:

   a. Aceda ao modo de privilégio avançado e introduza y quando lhe for pedido para continuar:

      ```
      set priv advanced
      ```

   b. Atualizar propriedade do disco:

      ```
      disk refresh-ownership controller-name
      ```

   c. Voltar ao modo de administração:

      ```
      set priv admin
      ```

9. Espelhe os agregados de raiz para node_A_2-IP e node_B_2-IP:

   ```
   aggregate mirror -aggregate root-aggr
   ```

10. Verifique se a re-sincronização de agregados foi concluída para agregados de raiz e dados:

    ```
    aggr show``aggr plex show
    ```

    A ressincronização pode demorar algum tempo, mas deve ser concluída antes de prosseguir com as

etapas a seguir.

11. Atualize a configuração do MetroCluster para incorporar os novos nós:
    a. Aceda ao modo de privilégio avançado e introduza y quando lhe for pedido para continuar:

       ```
       set priv advanced
       ```

    b. Atualizar a configuração:

Se tiver configurado…	Emitir este comando…
Um único agregado em cada cluster:	`metrocluster configure -refresh true -allow-with-one-aggregate true`
Mais de um único agregado em cada cluster	`metrocluster configure -refresh true`

    c. Voltar ao modo de administração:

       ```
       set priv admin
       ```

12. Desativar o modo de transição MetroCluster:
    a. Entre no modo de privilégio avançado e digite "'y'" quando solicitado a continuar:

       ```
       set priv advanced
       ```

    b. Desativar modo de transição:

       ```
       metrocluster transition disable
       ```

    c. Voltar ao modo de administração:

       ```
       set priv admin
       ```

Configuração de LIFs de dados nos novos nós

Você deve configurar LIFs de dados nos novos nós, node_A_2-IP e node_B_2-IP.

Você deve adicionar novas portas disponíveis em novos controladores a um domínio de broadcast se ainda não estiver atribuído a um. Se necessário, crie VLANs ou grupos de interface nas novas portas. Consulte "Gerenciamento de rede"

1. Identificar o uso atual da porta e os domínios de broadcast:

   ```
   network port show``network port broadcast-domain show
   ```

2. Adicione portas a domínios de broadcast e VLANs conforme necessário.
    a. Visualizar os espaços IP:

       ```
       network ipspace show
       ```

b. Crie espaços IP e atribua portas de dados conforme necessário.

"Configurando IPspaces (somente administradores de cluster)"

c. Veja os domínios de broadcast:

```
network port broadcast-domain show
```

d. Adicione todas as portas de dados a um domínio de broadcast conforme necessário.

"Adicionar ou remover portas de um domínio de broadcast"

e. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

3. Verifique se os LIFs estão hospedados no nó apropriado e nas portas nos nós IP do MetroCluster (incluindo o SVM com -mc vserver), conforme necessário.

Consulte as informações reunidas em "Criando a configuração de rede".

a. Verifique a porta inicial dos LIFs:

```
network interface show -field home-port
```

b. Se necessário, modifique a configuração de LIF:

```
vserver config override -command "network interface modify -vserver
<svm_name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>
```

c. Reverter os LIFs para suas portas residenciais:

```
network interface revert * -vserver <svm_name>
```

Trazendo os SVMs

Devido às alterações na configuração de LIF, você deve reiniciar os SVMs nos novos nós.

Passos

1. Verifique o estado das SVMs:

```
metrocluster vserver show
```

2. Reinicie os SVMs no cluster_A que não tenham um sufixo "'-mc":

```
vserver start -vserver <svm_name> -force true
```

3. Repita as etapas anteriores no cluster de parceiros.

4. Verifique se todos os SVMs estão em um estado saudável:

   ```
   metrocluster vserver show
   ```

5. Verifique se todas as LIFs de dados estão online:

   ```
   network interface show
   ```

Mover um volume de sistema para os novos nós

Para melhorar a resiliência, um volume do sistema deve ser movido do nó do controlador_A_1-IP para o nó do controlador_A_2-IP e também do nó_B_1-IP para o nó_B_2-IP. Você deve criar um agregado espelhado no nó de destino para o volume do sistema.

Sobre esta tarefa

Os volumes do sistema têm o nome "MDV"*CRS*A" ou "MDV_CRS*B." as designações ""_A" e ""_B" não estão relacionadas com as referências site_A e site_B usadas ao longo desta seção; por exemplo, MDV_CRS*_A não está associado com site_A.

Passos

1. Atribua pelo menos três discos de pool 0 e três de pool 1 cada um para controladores node_A_2-IP e node_B_2-IP conforme necessário.
2. Ative a atribuição automática do disco.
3. Mova o volume do sistema _B de node_A_1-IP para node_A_2-IP usando as etapas a seguir de site_A.

   a. Crie um agregado espelhado no controlador node_A_2-IP para manter o volume do sistema:

      ```
      aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node
      node_A_2-IP

      aggr show
      ```

      O agregado espelhado requer cinco discos sobressalentes do pool 0 e cinco do pool 1 de propriedade do controller node_A_2-IP.

      A opção avançada, "'-force-small-Aggregate True" pode ser usada para limitar o uso de disco a 3 discos pool 0 e 3 discos pool 1, se os discos estiverem em suprimento curto.

   b. Listar os volumes do sistema associados ao SVM de administrador:

      ```
      vserver show

      volume show -vserver <admin_svm_name>
      ```

   Você deve identificar volumes contidos por agregados de propriedade do site_A. Os volumes do sistema site_B também serão exibidos.

4. Mova o volume do sistema MDV_CRS_*_B para site_A para o agregado espelhado criado no controlador node_A_2-IP

   a. Verifique possíveis agregados de destino:

```
volume move target-aggr show -vserver <admin_svm_name> -volume MDV_CRS_*_B
```

O agregado recém-criado em node_A_2-IP deve ser listado.

b. Mova o volume para o agregado recém-criado no node_A_2-IP:

```
set advanced

volume move start -vserver <admin_svm_name> -volume MDV_CRS_*_B -destination
-aggregate new_node_A_2-IP_aggr -cutover-window 40
```

c. Verifique o estado da operação de deslocação:

```
volume move show -vserver <admin_svm_name> -volume MDV_CRS_*_B
```

d. Quando a operação mover estiver concluída, verifique se o sistema MDV_CRS_*_B está contido pelo novo agregado no node_A_2-IP:

```
set admin

volume show -vserver <admin_svm_name>
```

5. Repita as etapas acima no site_B (node_B_1-IP e node_B_2-IP).

Voltar a colocar o sistema em funcionamento normal

Você deve executar as etapas finais de configuração e retornar a configuração do MetroCluster à operação normal.

Verificando a operação do MetroCluster e atribuindo unidades após a transição

Você deve verificar se o MetroCluster está funcionando corretamente e atribuir unidades ao segundo par de novos nós (node_A_2-IP e node_B_2-IP).

1. Confirme se o tipo de configuração do MetroCluster é IP-Fabric: `metrocluster show`
2. Execute uma verificação MetroCluster.
   a. Emita o seguinte comando: `metrocluster check run`
   b. Apresentar os resultados da verificação MetroCluster: `metrocluster check show`
3. Confirme se o grupo de DR com os nós IP do MetroCluster está configurado: `metrocluster node show`
4. Criar e espelhar agregados de dados adicionais para controladores node_A_2-IP e node_B_2-IP em cada local conforme necessário.

Instalar licenças para o novo módulo de controlador

É necessário adicionar licenças para o novo módulo de controladora para quaisquer serviços ONTAP que exijam licenças padrão (node-locked). Para recursos com licenças padrão, cada nó no cluster deve ter sua própria chave para o recurso.

Para obter informações detalhadas sobre licenciamento, consulte o artigo 3013749 da base de conhecimento: Visão geral e referências de licenciamento do Data ONTAP 8.2 no site de suporte da NetApp e na *Referência*

de administração do sistema.

1. Se necessário, obtenha chaves de licença para o novo nó no site de suporte da NetApp na seção meu suporte em licenças de software.

   Para obter mais informações sobre substituições de licenças, consulte o artigo da base de dados de Conhecimento "Pós-processo de substituição da placa-mãe para atualizar o licenciamento em um sistema AFF/FAS."

2. Execute o seguinte comando para instalar cada chave de licença: `system license add -license -code license_key`

   A license_key tem 28 dígitos.

   Repita este passo para cada licença padrão (node-locked) necessária.

Concluir a configuração dos nós

Existem várias etapas de configuração que podem ser executadas antes de concluir os procedimentos. Alguns destes passos são opcionais.

1. Configure o processador de serviço: `system service-processor network modify`
2. Configure o AutoSupport nos novos nós: `system node autosupport modify`
3. Os controladores podem ser opcionalmente renomeados como parte da transição. O seguinte comando é usado para renomear um controlador: `system node rename -node <old-name> -newname <new-name>`

   A operação de renomeação pode levar alguns minutos para ser concluída. Confirme se quaisquer alterações de nome se propagaram para cada nó antes de continuar com outras etapas usando o comando system show -fields node.

4. Configure um serviço de monitoramento conforme desejado.

   "Considerações para Mediator"

   xref:./transition/./install-ip/concept_mediator_requirements.html

   "Instalação e configuração do software tiebreaker"

Enviar uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a transição, você deve enviar uma mensagem AutoSupport indicando o fim da manutenção, para que a criação automática de casos possa ser retomada.

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.
   a. Emita o seguinte comando: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repita o comando no cluster de parceiros.

Transição do MetroCluster FC para o MetroCluster IP sem interrupções ao desativar as gavetas de storage (ONTAP 9.8 e posterior)

A partir do ONTAP 9.8, você pode fazer a transição de uma configuração de FC MetroCluster de dois nós para uma configuração IP MetroCluster de quatro nós e desativar as gavetas de storage existentes. O procedimento inclui etapas para mover dados dos compartimentos de unidades existentes para a nova configuração e desativar as gavetas antigas.

- Esse procedimento é usado quando você planeja desativar os compartimentos de storage existentes e mover todos os dados para as novas gavetas na configuração IP do MetroCluster.
- Os modelos de gaveta de storage existentes devem ser compatíveis com os novos nós IP do MetroCluster.
- Este procedimento é suportado em sistemas que executam o ONTAP 9.8 e posterior.
- Este procedimento é disruptivo.
- Esse procedimento se aplica apenas a uma configuração de FC MetroCluster de dois nós.

  Se você tiver uma configuração de FC MetroCluster de quatro nós, "Escolhendo seu procedimento de transição"consulte .

- Você deve atender a todos os requisitos e seguir todas as etapas do procedimento.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Requisitos para a transição ao retirar prateleiras antigas

Antes de iniciar o processo de transição, certifique-se de que a configuração MetroCluster FC existente atenda aos requisitos.

- Ele precisa ser uma configuração de MetroCluster elástico ou conectado à malha de dois nós e todos os nós precisam estar executando o ONTAP 9.8 ou posterior.

  Os novos módulos do controlador IP MetroCluster devem estar executando a mesma versão do ONTAP 9.8.

- As plataformas existentes e novas devem ser uma combinação suportada para a transição.

  "Plataformas compatíveis para transição sem interrupções"

- Ele deve atender a todos os requisitos e cabeamento, conforme descrito em *Guias de Instalação e Configuração do MetroCluster*.

  "Instalação e configuração do MetroCluster conectado à malha"

A nova configuração também deve atender aos seguintes requisitos:

- Os novos modelos de plataforma IP MetroCluster devem ser compatíveis com os modelos de gaveta de storage antigos.

  "NetApp Hardware Universe"

- Dependendo dos discos sobressalentes disponíveis nas gavetas existentes, é necessário adicionar unidades adicionais.

  Isso pode exigir gavetas de unidade adicionais.

  Você precisa ter 14 a 18 unidades adicionais para cada controlador:

  - Três unidades de pool de 0 TB
  - Três unidades de pool de 1 TB
  - Duas unidades de reserva
  - Seis a dez unidades para o volume do sistema

- Você deve garantir que a configuração, incluindo os novos nós, não exceda os limites da plataforma para a configuração, incluindo contagem de unidades, capacidade de tamanho de agregado raiz, etc.

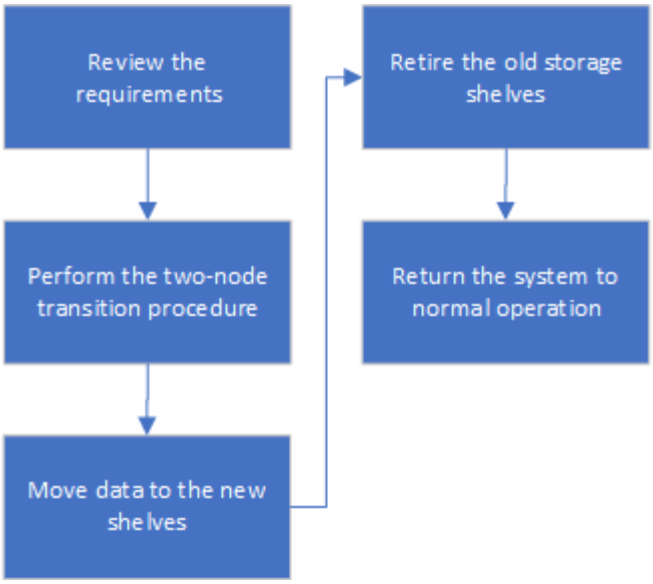
  Esta informação está disponível para cada modelo de plataforma em "NetApp Hardware Universe"

Você precisa ter acesso remoto ao console para todos os seis nós do site MetroCluster ou Planejar a viagem entre os locais conforme necessário pelo procedimento.

Fluxo de trabalho para transição disruptiva ao mover dados e desativar compartimentos de storage antigos

Você deve seguir o fluxo de trabalho específico para garantir uma transição bem-sucedida.

Enquanto você se prepara para a transição, Planeje viagens entre os sites. Observe que depois que os nós remotos forem colocados em rack e cabeados, você precisará ter acesso ao terminal serial aos nós. O acesso ao processador de serviço não estará disponível até que os nós sejam configurados.



Fazendo a transição da configuração

Você deve seguir o procedimento detalhado de transição.

Sobre esta tarefa

Nas etapas a seguir, você será direcionado a outros procedimentos. Você deve executar as etapas em cada procedimento referenciado na ordem indicada.

Passos

1. Planeje o mapeamento de portas usando as etapas em "Mapeamento de portas dos nós FC do MetroCluster para os nós IP do MetroCluster".
2. Prepare os controladores IP do MetroCluster usando as etapas em "Preparação dos controladores IP MetroCluster".
3. Verifique a integridade da configuração do MetroCluster FC.

   Execute as etapas em "Verificando a integridade da configuração do MetroCluster FC".

4. Colete informações da configuração do MetroCluster FC.

   Execute as etapas em "Recolha de informações dos módulos do controlador existentes antes da transição".

5. Remova a monitorização do desempate, se necessário.

   Execute as etapas em "Remoção da configuração existente do tiebreaker ou de outro software de monitoramento".

6. Preparar e remover os nós FC do MetroCluster existentes.

   Execute as etapas em "Fazendo a transição dos nós do MetroCluster FC".

7. Conete os novos nós IP do MetroCluster.

   Execute as etapas em "Ligar os módulos do controlador IP MetroCluster".

8. Configure os novos nós IP do MetroCluster e conclua a transição.

Execute as etapas em "Configurar os novos nós e concluir a transição".

Migrando os agregados raiz

Após a conclusão da transição, migre os agregados de raiz existentes que sobraram da configuração MetroCluster FC para novas gavetas na configuração MetroCluster IP.

Sobre esta tarefa

Essa tarefa move os agregados raiz para node_A_1-FC e node_B_1-FC para compartimentos de disco pertencentes às novas controladoras IP MetroCluster:

Passos

1. Atribuir discos do pool 0 no novo compartimento de armazenamento local à controladora que tem a raiz sendo migrada (por exemplo, se a raiz do node_A_1-FC estiver sendo migrada, atribua discos do pool 0 no novo compartimento a node_A_1-IP)

   Observe que a migração *remove e não cria novamente o espelho raiz*, portanto, os discos do pool 1 não precisam ser atribuídos antes de emitir o comando Migrate

2. Defina o modo de privilégio como avançado:

   ```
   set priv advanced
   ```

3. Migrar o agregado raiz:

   ```
   system node migrate-root -node node-name -disklist disk-id1,disk-id2,diskn
   -raid-type raid-type
   ```

   - O nome do nó é o nó para o qual o agregado raiz está sendo migrado.
   - O ID do disco identifica os discos do pool 0 na nova gaveta.
   - O tipo raid normalmente é o mesmo que o tipo raid do agregado raiz existente.
   - Você pode usar o comando `job show -idjob-id-instance` para verificar o status da migração, em que o id da tarefa é o valor fornecido quando o comando migrate-root é emitido.

     Por exemplo, se o agregado raiz para node_A_1-FC consistia em três discos com raid_dp, o seguinte comando seria usado para migrar raiz para um novo shelf 11:

   ```
   system node migrate-root -node node_A_1-IP -disklist
   3.11.0,3.11.1,3.11.2 -raid-type raid_dp
   ```

4. Aguarde até que a operação de migração seja concluída e o nó seja reinicializado automaticamente.
5. Atribua discos do pool 1 para o agregado raiz em um novo compartimento diretamente conetado ao cluster remoto.
6. Espelhar o agregado raiz migrado.
7. Aguarde até que o agregado raiz conclua a ressincronização.

   Você pode usar o comando storage Aggregate show para verificar o status de sincronização dos agregados.

8. Repita essas etapas para o outro agregado de raiz.

Migração dos agregados de dados

Criar agregados de dados nas novas gavetas e usar a movimentação de volume para transferir os volumes de dados das prateleiras antigas para os agregados nas novas gavetas.

1. Mova os volumes de dados para agregados nas novas controladoras, um volume de cada vez.

   "Criando um agregado e movendo volumes para os novos nós"

A remoção de compartimentos foi movida de node_A_1-FC e node_A_2-FC

Remova as gavetas de storage antigas da configuração original do MetroCluster FC. Essas gavetas eram originalmente propriedade de node_A_1-FC e node_A_2-FC.

1. Identifique os agregados nas prateleiras antigas no cluster_B que precisam ser excluídos.

   Neste exemplo, os seguintes agregados de dados são hospedados pelo cluster_B do MetroCluster FC e precisam ser excluídos: aggr_data_A1 e aggr_data_A2.

   Você precisa executar as etapas para identificar, off-line e excluir os agregados de dados nas gavetas. O exemplo é apenas para um cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-IP
raid_dp,

mirrored,

normal
aggr0_node_A_2-IP
           349.0GB   16.83GB   95% online       1 node_A_2-IP
raid_dp,

mirrored,

normal
...
8 entries were displayed.

cluster_B::>
```

2. Verifique se os agregados de dados têm quaisquer volumes MDV_aud e elimine-os antes de eliminar os agregados.

   Você deve excluir os volumes MDV_aud porque eles não podem ser movidos.

3. Coloque cada um dos agregados offline e, em seguida, exclua-os:

   a. Coloque o agregado off-line:

      `storage aggregate offline -aggregate aggregate-name`

      O exemplo a seguir mostra o nó agregado_B_1_aggr0 sendo colocado off-line:

      ```
      cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

      Aggregate offline successful on aggregate: node_B_1_aggr0
      ```

   b. Eliminar o agregado:

      `storage aggregate delete -aggregate aggregate-name`

      Você pode destruir o Plex quando solicitado.

O exemplo a seguir mostra o nó agregado_B_1_aggr0 sendo excluído.

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. Depois de excluir todos os agregados, desligue, desconete e remova as gavetas.
5. Repita as etapas acima para desativar as prateleiras cluster_A.

Concluir a transição

Com os módulos de controlador antigos removidos, você pode concluir o processo de transição.

Passo

1. Conclua o processo de transição.

   Execute as etapas em "Voltar a colocar o sistema em funcionamento normal".

Transição sem interrupções quando as gavetas atuais não são compatíveis com novos controladores (ONTAP 9.8 e posterior)

A partir do ONTAP 9.8, você pode fazer a transição de uma configuração de FC MetroCluster de dois nós e mover dados das gavetas de unidades existentes, mesmo que as gavetas de storage existentes não sejam suportadas pelos novos nós IP do MetroCluster.

- Este procedimento só deve ser usado se os modelos de prateleiras de armazenamento existentes não forem suportados pelos novos modelos de plataforma IP MetroCluster.
- Este procedimento é suportado em sistemas que executam o ONTAP 9.8 e posterior.
- Este procedimento é disruptivo.
- Esse procedimento se aplica apenas a uma configuração de FC MetroCluster de dois nós.

  Se você tiver uma configuração de FC MetroCluster de quatro nós, "Escolhendo seu procedimento de transição"consulte .

- Você deve atender a todos os requisitos e seguir todas as etapas do procedimento.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Requisitos de transição quando as gavetas não são compatíveis com os novos nós

Antes de iniciar o processo de transição, você deve garantir que a configuração atenda aos requisitos.

Antes de começar

- A configuração existente deve ser uma configuração de MetroCluster alongada ou conectada à malha de dois nós e todos os nós precisam estar executando o ONTAP 9.8 ou posterior.

  Os novos módulos do controlador IP MetroCluster devem estar executando a mesma versão do ONTAP 9.8.

- As plataformas existentes e novas devem ser uma combinação suportada para a transição.

  "Plataformas compatíveis para transição sem interrupções"

- Ele deve atender a todos os requisitos e cabeamento, conforme descrito "Instalação e configuração do MetroCluster conectado à malha"em .
- Os novos compartimentos de storage fornecidos com os novos controladores (node_A_1-IP, node_A_2-IP, node_B_1-IP e node_B_2-IP) devem ser suportados pelos controladores antigos (node_A_1-FC e node_B_1-FC).

  "NetApp Hardware Universe"

- As prateleiras de armazenamento antigas são **não** suportadas pelos novos modelos de plataforma IP MetroCluster.

  "NetApp Hardware Universe"

- Dependendo dos discos sobressalentes disponíveis nas gavetas existentes, é necessário adicionar unidades adicionais.

  Isso pode exigir gavetas de unidade adicionais.

  Você precisa ter 14 a 18 unidades adicionais para cada controlador:

  - Três unidades de pool0 TB
  - Três unidades de pool1 TB
  - Duas unidades de reserva
  - Seis a dez unidades para o volume do sistema
- Você deve garantir que a configuração, incluindo os novos nós, não exceda os limites da plataforma para

a configuração, incluindo contagem de unidades, capacidade de tamanho de agregado raiz, etc.

Esta informação está disponível para cada modelo de plataforma em *NetApp Hardware Universe*.

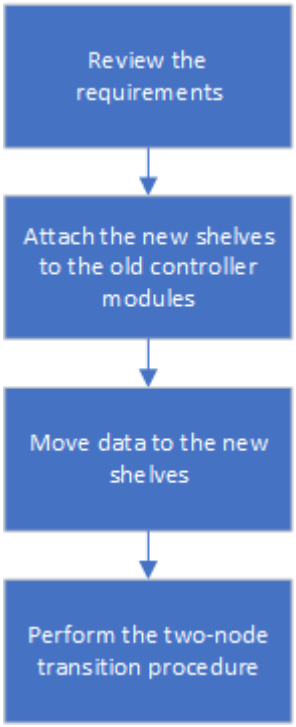
"NetApp Hardware Universe"

- Você precisa ter acesso remoto ao console para todos os seis nós do site MetroCluster ou Planejar a viagem entre os locais conforme necessário pelo procedimento.

Fluxo de trabalho para transição disruptiva quando as gavetas não são suportadas por novas controladoras

Se os modelos de gaveta existentes não forem compatíveis com os novos modelos de plataforma, você precisará anexar as novas gavetas à configuração antiga, mover dados para as novas gavetas e depois fazer a transição para a nova configuração.

Enquanto você se prepara para a transição, Planeje viagens entre os sites. Observe que depois que os nós remotos forem colocados em rack e cabeados, você precisará ter acesso ao terminal serial aos nós. O acesso ao processador de serviço não estará disponível até que os nós sejam configurados.



Preparar os novos módulos do controlador

Você precisa limpar a configuração e a propriedade de disco nos novos módulos de controladora e nos novos compartimentos de storage.

Passos

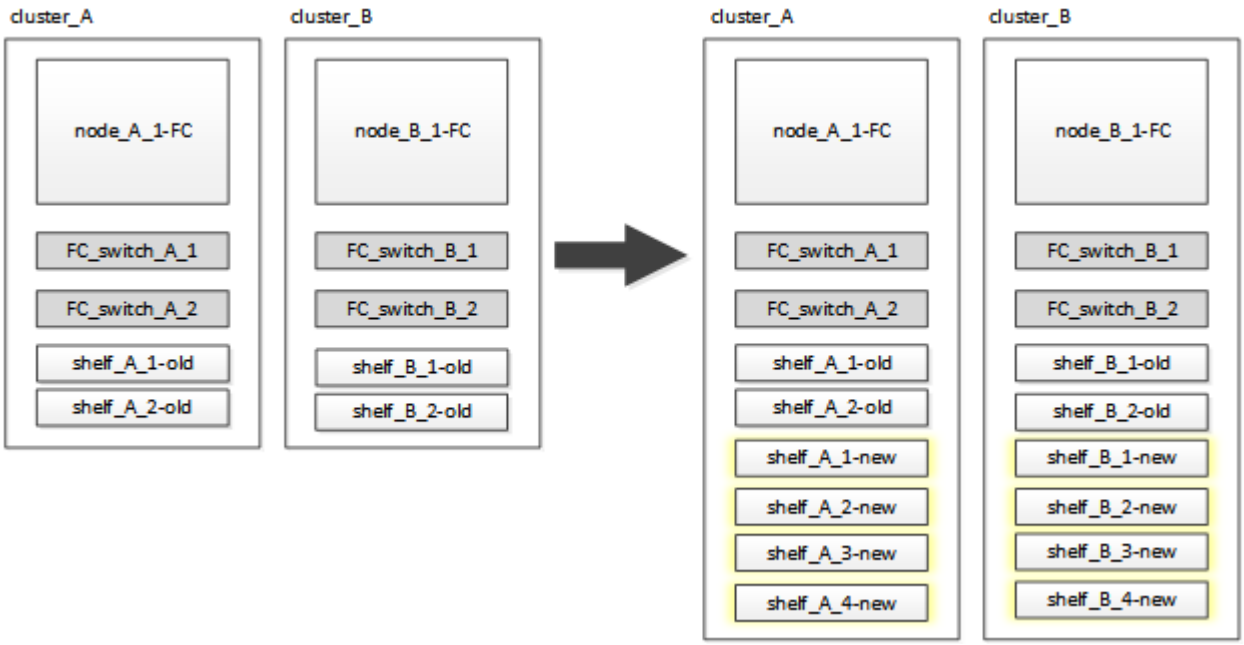
1. Com os novos compartimentos de armazenamento conetados aos novos módulos de controladora IP do MetroCluster, execute todas as etapas em "Preparação dos controladores IP MetroCluster".
2. Desconete os novos compartimentos de storage dos novos módulos de controladora IP MetroCluster.

Anexando os novos compartimentos de disco às controladoras MetroCluster FC existentes

É necessário anexar os novos compartimentos de unidades aos módulos de controladora existentes antes de fazer a transição para uma configuração IP do MetroCluster.

Sobre esta tarefa

A ilustração a seguir mostra as novas gavetas conetadas à configuração do MetroCluster FC.



Passos

1. Desative a atribuição automática de disco em node_A_1-FC e node_A_2-FC:

   `disk option modify -node` *`node-name`* `-autoassign off`

   Este comando deve ser emitido em cada nó.

   A atribuição automática de disco está desativada para evitar a atribuição das gavetas a serem adicionadas ao node_A_1-FC e node_B_1-FC. Como parte da transição, os discos são necessários para nós node_A_1-IP e node_B_2-IP e se a atribuição automática for permitida, a propriedade do disco precisaria ser removida mais tarde antes que os discos pudessem ser atribuídos a node_A_1-IP e node_B_2-IP.

2. Conecte as novas gavetas aos nós FC do MetroCluster existentes, usando pontes FC para SAS, se necessário.

   Consulte os requisitos e procedimentos em "Storage de adição automática a uma configuração MetroCluster FC"

Migre agregados de raiz e migre dados para as novas gavetas de disco

É necessário mover os agregados raiz das gavetas de unidade antigas para as novas gavetas de unidade que serão usadas pelos nós IP do MetroCluster.

Sobre esta tarefa

Essa tarefa é executada antes da transição nos nós existentes (node_A_1-FC e node_B_1-FC).

Passos

1. Execute um switchover negociado a partir do nó do controlador_B_1-FC:

   ```
   metrocluster switchover
   ```

2. Execute as etapas de heal Aggregates e heal root da recuperação de node_B_1-FC:

   ```
   metrocluster heal -phase aggregates

   metrocluster heal -phase root-aggregates
   ```

3. Controlador de arranque node_A_1-FC:

   ```
   boot_ontap
   ```

4. Atribua os discos não pertencentes às novas gavetas aos pools apropriados para o nó do controlador_A_1-FC:

   a. Identifique os discos nas gavetas:

      ```
      disk show -shelf pool_0_shelf -fields container-type,diskpathnames

      disk show -shelf pool_1_shelf -fields container-type,diskpathnames
      ```

   b. Entre no modo local para que os comandos sejam executados no nó local:

      ```
      run local
      ```

   c. Atribuir os discos:

      ```
      disk assign disk1disk2disk3disk… -p 0

   disk assign disk4disk5disk6disk… -p 1
      ```

   a. Sair do modo local:

      ```
      exit
      ```

5. Crie um novo agregado espelhado para se tornar o novo agregado de raiz para o node_A_1-FC do controlador:

   a. Defina o modo de privilégio como avançado:

      ```
      set priv advanced
      ```

   b. Criar o agregado:

      ```
      aggregate create -aggregate new_aggr -disklist disk1, disk2, disk3,… -mirror
      -disklist disk4disk5, disk6,… -raidtypesame-as-existing-root -force-small
      -aggregate true aggr show -aggregate new_aggr -fields percent-snapshot-space
      ```

      Se o valor percentual de espaço instantâneo for inferior a 5 por cento, você deve aumentá-lo para um valor superior a 5 por cento:

```
aggr modify new_aggr -percent-snapshot-space 5
```

a. Defina o modo de privilégio de volta para admin:

```
set priv admin
```

6. Confirme se o novo agregado foi criado corretamente:

```
node run -node local sysconfig -r
```

7. Crie os backups de configuração em nível de cluster e nó:

> Quando os backups são criados durante o switchover, o cluster está ciente do estado de comutação na recuperação. Você deve garantir que o backup e o upload da configuração do sistema sejam bem-sucedidos, pois sem esse backup é **não** possível reformar a configuração do MetroCluster entre clusters.

a. Criar a cópia de segurança do cluster:

```
system configuration backup create -node local -backup-type cluster -backup
-name cluster-backup-name
```

b. Verifique a criação da cópia de segurança do cluster

```
job show -id job-idstatus
```

c. Crie o backup do nó:

```
system configuration backup create -node local -backup-type node -backup
-name node-backup-name
```

d. Verifique se há backups de nós e de cluster:

```
system configuration backup show
```

Você pode repetir o comando até que ambos os backups sejam exibidos na saída.

8. Faça cópias dos backups.

Os backups devem ser armazenados em um local separado porque serão perdidos localmente quando o novo volume raiz for inicializado.

Você pode fazer o upload dos backups para um servidor FTP ou HTTP ou copiar os backups usando `scp` comandos.

Processo	Passos

Carregue o backup para o servidor FTP ou HTTP	a. Carregar a cópia de segurança do cluster: `system configuration backup upload -node local -backup` *`cluster-backup-name`* `-destination URL` b. Carregue a cópia de segurança do nó: `system configuration backup upload -node local -backup` *`node-backup-name`* `-destination URL`
Copie os backups em um servidor remoto usando cópia segura	A partir do servidor remoto use os seguintes comandos scp: a. Copiar a cópia de segurança do cluster: `scp diagnode-mgmt-FC:/mroot/etc/backups/config/cluster-backup-name.7z .` b. Copie o backup do nó: `scp diag@node-mgmt-FC:/mroot/etc/backups/config/node-backup-name.7z .`

9. Halt node_A_1-FC:

   `halt -node local -ignore-quorum-warnings true`

10. Boot node_A_1-FC para o modo de manutenção:

    `boot_ontap maint`

11. No modo Manutenção, faça as alterações necessárias para definir o agregado como raiz:

    a. Defina a política de HA para cfo:

       `aggr options new_aggr ha_policy cfo`

       Responda "sim" quando solicitado a prosseguir.

    ```
    Are you sure you want to proceed (y/n)?
    ```

    a. Defina o novo agregado como raiz:

       `aggr options new_aggr root`

    b. Parar para o prompt Loader:

       `halt`

12. Inicialize o controlador e faça backup da configuração do sistema.

O nó é inicializado no modo de recuperação quando o novo volume raiz é detetado

a. Inicialize o controlador:

```
boot_ontap
```

b. Inicie sessão e faça uma cópia de segurança da configuração.

Ao iniciar sessão, verá o seguinte aviso:

```
Warning: The correct cluster system configuration backup must be
restored. If a backup
from another cluster or another system state is used then the root
volume will need to be
recreated and NGS engaged for recovery assistance.
```

a. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

b. Faça backup da configuração do cluster para um servidor:

```
system configuration backup download -node local -source URL of
server/cluster-backup-name.7z
```

c. Faça backup da configuração do nó em um servidor:

```
system configuration backup download -node local -source URL of server/node-
backup-name.7z
```

d. Voltar ao modo de administração:

```
set -privilege admin
```

13. Verifique a integridade do cluster:

a. Emita o seguinte comando:

```
cluster show
```

b. Defina o modo de privilégio como avançado:

```
set -privilege advanced
```

c. Verifique os detalhes da configuração do cluster:

```
cluster ring show
```

d. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

14. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
    a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

       ```
       metrocluster show
       ```

    b. Confirme se todos os nós esperados são mostrados:

       ```
       metrocluster node show
       ```

    c. Emita o seguinte comando:

       ```
       metrocluster check run
       ```

    d. Apresentar os resultados da verificação MetroCluster:

       ```
       metrocluster check show
       ```

15. Execute um switchback do nó_B_1-FC do controlador:

    ```
    metrocluster switchback
    ```

16. Verifique o funcionamento da configuração do MetroCluster:
    a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

       ```
       metrocluster show
       ```

    b. Execute uma verificação MetroCluster:

       ```
       metrocluster check run
       ```

    c. Apresentar os resultados da verificação MetroCluster:

       ```
       metrocluster check show
       ```

17. Adicione o novo volume raiz à base de dados de localização de volume.
    a. Defina o modo de privilégio como avançado:

       ```
       set -privilege advanced
       ```

    b. Adicione o volume ao nó:

       ```
       volume add-other-volumes –node node_A_1-FC
       ```

    c. Voltar ao nível de privilégio de administrador:

       ```
       set -privilege admin
       ```

18. Verifique se o volume está agora visível e tem mroot.
    a. Exibir os agregados:

       ```
       storage aggregate show
       ```

b. Verifique se o volume raiz tem mroot:

```
storage aggregate show -fields has-mroot
```

c. Apresentar os volumes:

```
volume show
```

19. Crie um novo certificado de segurança para reativar o acesso ao System Manager:

```
security certificate create -common-name name -type server -size 2048
```

20. Repita as etapas anteriores para migrar os agregados nas gavetas de propriedade de node_A_1-FC.
21. Execute uma limpeza.

Você deve executar as etapas a seguir em node_A_1-FC e node_B_1-FC para remover o volume raiz antigo e o agregado raiz.

a. Exclua o volume raiz antigo:

```
run local

vol offline old_vol0

vol destroy old_vol0

exit

volume remove-other-volume -vserver node_name -volume old_vol0
```

b. Excluir o agregado raiz original:

```
aggr offline -aggregate old_aggr0_site
```

```
aggr delete -aggregate old_aggr0_site
```

22. Migre os volumes de dados para agregados nas novas controladoras, um volume de cada vez.

Consulte "Criando um agregado e movendo volumes para os novos nós"

23. Retire as prateleiras antigas executando todas as etapas em "A remoção de compartimentos foi movida de node_A_1-FC e node_A_2-FC".

Fazendo a transição da configuração

Você deve seguir o procedimento detalhado de transição.

Sobre esta tarefa

Nas etapas a seguir, você será direcionado para outros tópicos. Você deve executar as etapas em cada tópico na ordem dada.

Passos

1. Planear mapeamento de portas.

Execute todas as etapas em "Mapeamento de portas dos nós FC do MetroCluster para os nós IP do MetroCluster".

2. Prepare os controladores IP do MetroCluster.

   Execute todas as etapas em "Preparação dos controladores IP MetroCluster".

3. Verifique a integridade da configuração do MetroCluster.

   Execute todas as etapas em "Verificando a integridade da configuração do MetroCluster FC".

4. Preparar e remover os nós FC do MetroCluster existentes.

   Execute todas as etapas em "Fazendo a transição dos nós do MetroCluster FC".

5. Adicione os novos nós IP do MetroCluster.

   Execute todas as etapas em "Ligar os módulos do controlador IP MetroCluster".

6. Conclua a transição e a configuração inicial dos novos nós IP do MetroCluster.

   Execute todas as etapas em "Configurar os novos nós e concluir a transição".

Movimentação de um workload de FC SAN do MetroCluster FC para os nós IP do MetroCluster

Ao fazer a transição do MetroCluster FC para nós IP sem interrupções, você precisa mover objetos de host FC SAN do MetroCluster FC para nós IP sem interrupções.

Mover um workload de FC SAN do MetroCluster FC para os nós IP do MetroCluster

Passos

1. Configure novas interfaces FC (LIFS) em nós IP do MetroCluster:
   a. Se necessário, nos nós IP do MetroCluster, modifique as portas FC a serem usadas para a conectividade do cliente com a personalidade de destino FC.

      Isso pode exigir uma reinicialização dos nós.

   b. Crie FC LIFS/interfaces em nós IP para todos os SVMs SAN. Opcionalmente, verifique se os WWPNs de FC LIFs recém-criados estão conetados ao switch SAN FC
2. Atualize a configuração de zoneamento SAN para LIFs FC recém-adicionados em nós IP do MetroCluster.

   Para facilitar a movimentação de volumes que contêm LUNs que fornecem dados ativamente a clientes FC SAN, atualize as zonas de switch FC existentes para permitir que clientes FC SAN acessem LUNs nos nós IP do MetroCluster.

   a. No switch SAN FC (Cisco ou Brocade), adicione as WWPNs de LIFs SAN FC recém-adicionados à zona.
   b. Atualize, salve e confirme as alterações de zoneamento.
   c. No cliente, verifique se há logins do iniciador FC para os novos LIFs SAN nos nós IP do MetroCluster: `sanlun lun show -p`

Neste momento, o cliente deve ver e fazer login nas interfaces FC nos nós IP MetroCluster FC e MetroCluster. LUNs e volumes ainda ficam hospedados fisicamente nos nós de FC do MetroCluster.

Como os LUNs são relatados apenas nas interfaces de nó MetroCluster FC, o cliente mostra apenas caminhos em nós FC. Isto pode ser visto na saída dos `sanlun lun show -p` comandos e. `multipath -ll -d`

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

3. Modifique os nós de relatório para adicionar os nós IP do MetroCluster

   a. Listar nós de geração de relatórios de LUNs na SVM: `lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux`

      Os nós de geração de relatórios mostrados são nós locais, pois os LUNs estão fisicamente nos nós FC A_1 e A_2.

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                          igroup         reporting-nodes
-------  ----------------------------- ------------
-------------------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol1/lun_linux_3 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol2/lun_linux_4 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol3/lun_linux_7 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_8 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_9 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_12 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_13 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol7/lun_linux_14 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol8/lun_linux_17 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_18 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_19 igroup_linux  A_1,A_2
12 entries were displayed.
```

b. Adicione nós de relatório para incluir nós IP do MetroCluster.

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes B_1,B_2 -igroup igroup_linux

12 entries were acted on.
```

c. Listar nós de relatórios e verificar a presença dos novos nós:

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                            igroup          reporting-nodes
------- ------------------------------  ------------
-------------------------------------------------------------------------
----------

vsa_1   /vol/vsa_1_vol1/lun_linux_2   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol1/lun_linux_3   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol2/lun_linux_4   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol3/lun_linux_7   igroup_linux    A_1,A_2,B_1,B_2
...

12 entries were displayed.
```

d. Verifique se o `sg3-utils` pacote está instalado no host Linux. Isso evita um `rescan-scsi-bus.sh utility not found` erro quando você revê o host Linux para os LUNs recentemente mapeados usando o `rescan-scsi-bus` comando.

e. Volte a digitalizar o barramento SCSI no host para descobrir os caminhos recém-adicionados: `/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

f. Exiba os caminhos recém-adicionados: `sanlun lun show -p`

   Cada LUN terá quatro caminhos.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a0980383046465l3f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

g. Nas controladoras, mova os volumes que contêm LUNs do MetroCluster FC para os nós IP do MetroCluster.

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver    Volume    State    Move Phase   Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------   ---------------
----------------
vsa_1     vsa_1_vol1 healthy  initializing
 - -
```

h. No cliente SAN FC, exiba as informações de LUN: `sanlun lun show -p`

   As interfaces FC nos nós IP do MetroCluster onde o LUN agora reside são atualizadas como caminhos principais. Se o caminho primário não for atualizado após a movimentação do volume, execute /usr/bin/rescan-scsi-bus.sh -a ou simplesmente aguarde que o recurso multipath ocorra.

   O caminho principal no exemplo a seguir é o LIF no nó IP do MetroCluster.

```
[root@localhost ~]# sanlun lun show -p

                    ONTAP Path: vsa_1:/vol/vsa_1_vol1/lun_linux_2
                           LUN: 22
                      LUN Size: 2g
                       Product: cDOT
                   Host Device: 3600a098038302d324e5d50305063546e
              Multipath Policy: service-time 0
            Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      vserver
path      path       /dev/   host         vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------
----------------------------------------------
up        primary    sddv    host6        fc_5
up        primary    sdjx    host7        fc_6
up        secondary  sdgv    host6        fc_8
up        secondary  sdkr    host7        fc_8
```

a. Repita as etapas acima para todos os volumes, LUNs e interfaces FC pertencentes a um host SAN FC.

   Quando concluído, todos os LUNs de um determinado SVM e host FC SAN devem estar nos nós IP do MetroCluster.

4. Remova os nós de relatório e faça a varredura de caminhos do cliente.

   a. Remover os nós de geração de relatórios remotos (os nós FC do MetroCluster) para as LUNs linux: `lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igroup_linux -remote-nodes true`

   ```
   cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
   * -igroup igroup_linux -remote-nodes true
   12 entries were acted on.
   ```

   b. Verifique os nós de geração de relatórios para LUNs: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
------- --------------------------- ------------
----------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol2/lun_linux_4 igroup_linux B_1,B_2
...

12 entries were displayed.
```

c. Volte a digitalizar o barramento SCSI no cliente: `/usr/bin/rescan-scsi-bus.sh -r`

Os caminhos dos nós FC do MetroCluster são removidos:

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
...
```

a. Verifique se apenas os caminhos dos nós IP do MetroCluster estão visíveis a partir do host: `sanlun lun show -p`

b. Se necessário, remova iSCSI LIFs dos nós FC do MetroCluster.

   Isso deve ser feito se não houver outros LUNs nos nós mapeados para outros clientes.

Mova hosts iSCSI Linux do MetroCluster FC para nós IP MetroCluster

Depois de fazer a transição de seus nós MetroCluster do FC para o IP, talvez seja necessário mover suas conexões de host iSCSI para os novos nós.

Sobre esta tarefa

- As interfaces IPv4 são criadas quando você configura as novas conexões iSCSI.
- Os comandos e exemplos do host são específicos dos sistemas operacionais Linux.
- Os nós FC do MetroCluster são chamados de nós antigos e os nós IP do MetroCluster são chamados de nós novos.

Etapa 1: Configurar novas conexões iSCSI

Para mover as conexões iSCSI, configure novas conexões iSCSI para os novos nós.

Passos

1. Crie interfaces iSCSI nos novos nós e verifique a conetividade de ping dos hosts iSCSI para as novas interfaces nos novos nós.

   "Crie interfaces de rede"

   Todas as interfaces iSCSI do SVM devem ser acessíveis pelo host iSCSI.

2. No host iSCSI, identifique as conexões iSCSI existentes do host para o nó antigo:

   ```
   iscsiadm -m session
   ```

   ```
   [root@scspr1789621001 ~]# iscsiadm -m session
   tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   ```

3. No novo nó, verifique as conexões do novo nó:

   ```
   iscsi session show -vserver <svm-name>
   ```

```
node_A_1-new::*> iscsi session show -vserver vsa_1
 Tpgroup Initiator Initiator
Vserver Name TSIH Name ISID Alias
--------- ------- ---- ----------------------- ---------
--------------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
scspr1789621001.gdl.englab.netapp.com
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
scspr1789621001.gdl.englab.netapp.com
2 entries were displayed.
```

4. No novo nó, liste as interfaces iSCSI no ONTAP para o SVM que contém as interfaces:

```
iscsi interface show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1
 Logical Status Curr Curr
Vserver Interface  TPGT Admin/Oper IP Address Node Port Enabled
------- ---------- ---- ---------- --------------- ----------- ----
-------
vsa_1 iscsi_lf__n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
true
vsa_1 iscsi_lf__n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
htp-001 e0h true
vsa_1 iscsi_lf__n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
true
vsa_1 iscsi_lf__n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
htp-002 e0h true
vsa_1 iscsi_lf__n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
true
vsa_1 iscsi_lf__n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
true
6 entries were displayed.
```

5. No host iSCSI, execute a descoberta em qualquer um dos endereços IP iSCSI na SVM para descobrir os novos destinos:

```
iscsiadm -m discovery -t sendtargets -p iscsi-ip-address
```

A descoberta pode ser executada em qualquer endereço IP da SVM, incluindo interfaces não iSCSI.

```
[root@scspr1789621001 ~]# iscsiadm -m discovery -t sendtargets -p
10.230.68.236:3260
10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.134:3260,1183 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. No host iSCSI, faça login em todos os endereços descobertos:

```
iscsiadm -m node -L all -T node-address -p portal-address -l
```

```
[root@scspr1789621001 ~]# iscsiadm -m node -L all -T iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p
10.230.68.236:3260 -l
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] (multiple)
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] (multiple)
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] successful.
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] successful.
```

7. No host iSCSI, verifique o login e as conexões:

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. No novo nó, verifique o login e a conexão com o host:

```
iscsi initiator show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi initiator show -vserver vsa_1
 Tpgroup Initiator
Vserver Name             TSIH Name                  ISID
Igroup Name
------- --------         ---- --------------------- -----------------
-----------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf__n3_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf__n4_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux
4 entries were displayed.
```

Resultado

No final desta tarefa, o host pode ver todas as interfaces iSCSI (nos nós antigos e novos) e é conetado a todas essas interfaces.

LUNs e volumes ainda estão fisicamente hospedados nos nós antigos. Como os LUNs são relatados apenas nas interfaces de nó antigas, o host mostrará apenas caminhos sobre os nós antigos. Para ver isso, execute os `sanlun lun show -p` comandos e `multipath -ll -d` no host e examine as saídas de comando.

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ ------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------
up        primary    sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

Etapa 2: Adicione os novos nós como nós de relatório

Depois de configurar as conexões com os novos nós, você adiciona os novos nós como os nós de relatório.

Passos

1. No novo nó, liste nós de geração de relatórios de LUNs na SVM:

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   Os nós de relatórios a seguir são nós locais, pois LUNs estão fisicamente em nós antigos node_A_1-old e node_A_2-old.

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver path                          igroup       reporting-nodes
------- ----------------------------- ------------
---------------------------
vsa_1   /vol/vsa_1_vol1/lun_linux_2  igroup_linux node_A_1-old,node_A_2-
old
.
.
.
vsa_1   /vol/vsa_1_vol9/lun_linux_19 igroup_linux node_A_1-old,node_A_2-
old
12 entries were displayed.
```

2. No novo nó, adicione nós de relatório:

```
lun mapping add-reporting-nodes -vserver <svm-name> -path
/vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup <igroup_name>
```

```
node_A_1-new::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-new,node_A_2-new
-igroup igroup_linux
12 entries were acted on.
```

3. No novo nó, verifique se os nós recém-adicionados estão presentes:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux vserver path igroup reporting-nodes
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igroup reporting-nodes
------- -------------------------- ------------
-------------------------------------------------------------------------
-------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
.
.
.
12 entries were displayed.
```

4. O `sg3-utils` pacote deve ser instalado no host Linux. Isso evita um `rescan-scsi-bus.sh utility not found` erro quando você pode novamente o host Linux para os LUNs recentemente mapeados usando o `rescan-scsi-bus` comando.

   No host, verifique se o `sg3-utils` pacote está instalado:

   - Para uma distribuição baseada no Debian:

     ```
     dpkg -l | grep sg3-utils
     ```

   - Para uma distribuição baseada na Red Hat:

     ```
     rpm -qa | grep sg3-utils
     ```

   Se necessário, instale o `sg3-utils` pacote no host Linux:

   ```
   sudo apt-get install sg3-utils
   ```

5. No host, faça a varredura novamente do barramento SCSI no host e descubra os caminhos recém-adicionados:

   ```
   /usr/bin/rescan-scsi-bus.sh -a
   ```

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

6. No host iSCSI, liste os caminhos recém-adicionados:

```
sanlun lun show -p
```

Quatro caminhos são mostrados para cada LUN.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
------- ---------- ------- ----------- ---------------------
host vserver
path path /dev/ host vserver
state   type       node    adapter     LIF
------  ---------- ------- ----------- ---------------------
up      primary    sdk      host3      iscsi_lf__n2_p1_
up      secondary  sdh     host2       iscsi_lf__n1_p1_
up      secondary  sdag    host4       iscsi_lf__n4_p1_
up      secondary  sdah    host5       iscsi_lf__n3_p1_
```

7. No novo nó, mova o volume/volumes que contêm LUNs dos nós antigos para os novos nós.

```
node_A_1-new::*> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_vol1" command to view the status of this operation.
node_A_1-new::*> vol move show
Vserver  Volume      State       Move       Phase            Percent-
Complete  Time-To-Complete
-------- ----------  --------    ---------- ----------------
---------------  ----------------
vsa_1    vsa_1_vol1  healthy                initializing     -
-
```

8. Quando a movimentação do volume para os novos nós estiver concluída, verifique se o volume está online:

```
volume show -state
```

9. As interfaces iSCSI nos novos nós onde o LUN agora reside são atualizadas como caminhos primários. Se o caminho principal não for atualizado após a movimentação do volume, execute `/usr/bin/rescan-scsi-bus.sh -a` e `multipath -v3` no host ou simplesmente aguarde a nova varredura multipath ocorrer.

   No exemplo a seguir, o caminho primário é um LIF no novo nó.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ ----------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------------
up        primary    sdag    host4        iscsi_lf__n4_p1_
up        secondary  sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
up        secondary  sdah    host5        iscsi_lf__n3_p1_
```

Etapa 3: Remover nós de relatório e redigitalizar caminhos

Você deve remover os nós de relatório e verificar novamente os caminhos.

Passos

1. No novo nó, remova os nós de relatórios remotos (os novos nós) para as LUNs Linux:

```
lun mapping remove-reporting-nodes -vserver <svm-name> -path * -igroup
<igroup_name> -remote-nodes true
```

   Neste caso, os nós remotos são nós antigos.

```
node_A_1-new::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igroup_linux -remote-nodes true
12 entries were acted on.
```

2. No novo nó, verifique os nós de geração de relatórios das LUNs:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver  path                          igroup        reporting-nodes
-------  ----------------------------  ------------
-------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2  igroup_linux  node_A_1-
new,node_A_2-new
vsa_1    /vol/vsa_1_vol1/lun_linux_3  igroup_linux  node_A_1-
new,node_A_2-new
vsa_1    /vol/vsa_1_vol2/lun_linux_4  group_linux   node_A_1-
new,node_A_2-new
.
.
.
12 entries were displayed.
```

3. O `sg3-utils` pacote deve ser instalado no host Linux. Isso evita um `rescan-scsi-bus.sh utility not found` erro quando você pode novamente o host Linux para os LUNs recentemente mapeados usando o `rescan-scsi-bus` comando.

   No host, verifique se o `sg3-utils` pacote está instalado:

- Para uma distribuição baseada no Debian:

```
dpkg -l | grep sg3-utils
```

- Para uma distribuição baseada na Red Hat:

```
rpm -qa | grep sg3-utils
```

Se necessário, instale o `sg3-utils` pacote no host Linux:

```
sudo apt-get install sg3-utils
```

4. No host iSCSI, volte a digitalizar o barramento SCSI:

```
/usr/bin/rescan-scsi-bus.sh -r
```

Os caminhos que são removidos são os caminhos dos nós antigos.

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
.
.
.
```

5. No host iSCSI, verifique se apenas os caminhos dos novos nós estão visíveis:

```
sanlun lun show -p
```

```
multipath -ll -d
```

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto

"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster"	• Compreender a configuração do MetroCluster • Switchover, cura e switchback
"Recuperação de desastres"	• Recuperação de desastres • Comutação forçada • Recuperação de uma falha de vários controladores ou armazenamento
"Manutenção MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster FC • Procedimentos de substituição ou atualização de hardware e atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conetada à malha • Substituição de hardware em um local de desastre em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.

"Atualização e expansão do MetroCluster"	• Atualizando ou atualizando uma configuração do MetroCluster • Expansão de uma configuração do MetroCluster com a adição de nós adicionais
"Transição do MetroCluster"	• Transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP
"Atualização, transição e expansão do MetroCluster"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
"Documentação dos sistemas de hardware da ONTAP" **Nota:** os procedimentos de manutenção de prateleira de armazenamento padrão podem ser usados com configurações MetroCluster IP.	• Adição automática de um compartimento de disco • Remoção automática de um compartimento de disco
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
"Conceitos de ONTAP"	• Como os agregados espelhados funcionam

Atualize, atualize ou expanda a configuração do MetroCluster

Comece aqui - escolha o seu procedimento

Comece aqui: Escolha entre atualização do controlador, atualização do sistema ou expansão

Dependendo do escopo da atualização do equipamento, você escolhe um procedimento de atualização do controlador, um procedimento de atualização do sistema ou um procedimento de expansão.

- Os procedimentos de atualização do controlador aplicam-se apenas aos módulos do controlador. Os controladores são substituídos por um novo modelo de controlador.

  Os modelos de prateleiras de armazenamento não são atualizados.

  - Nos procedimentos de comutação e switchback, a operação de switchover do MetroCluster é usada para fornecer serviços sem interrupções aos clientes enquanto os módulos do controlador no cluster de parceiros são atualizados.
  - Em um procedimento de atualização de controladora baseado em ARL, as operações de realocação agregada são usadas para mover dados da configuração antiga para a configuração nova e atualizada sem interrupções.
- Os procedimentos de atualização se aplicam aos controladores e às gavetas de storage.

  Nos procedimentos de atualização, novos controladores e compartimentos são adicionados à configuração do MetroCluster, criando um segundo grupo de DR e migrando os dados para os novos nós sem interrupções.

  Os controladores originais são então desativados.
- Os procedimentos de expansão adicionam controladoras e gavetas adicionais à configuração do MetroCluster sem precisar remover.

  O procedimento utilizado depende do tipo de MetroCluster e do número de controladores existentes.

Tipo de atualização	Ir para…
Atualização da controladora	"Escolha um procedimento de atualização da controladora"
Atualização do sistema	"Escolha um procedimento de atualização do sistema"
Expansão	• "MetroCluster de dois nós para quatro" • "MetroCluster FC de quatro nós para oito" • "IP MetroCluster de quatro nós para oito"

Escolha um procedimento de atualização da controladora

O procedimento de atualização da controladora que você usa depende do modelo da plataforma e do tipo de configuração do MetroCluster.

Em um procedimento de atualização, os controladores são substituídos por um novo modelo de controlador. Os modelos de prateleiras de armazenamento não são atualizados.

- Nos procedimentos de comutação e switchback, a operação de switchover do MetroCluster é usada para fornecer serviços sem interrupções aos clientes enquanto os módulos do controlador no cluster de parceiros são atualizados.
- Em um procedimento de atualização de controladora baseado em ARL, as operações de realocação agregada são usadas para mover dados da configuração antiga para a configuração nova e atualizada sem interrupções.

Atualizações de controladora compatíveis

Saiba mais sobre as combinações de atualização de controladora FC e IP do MetroCluster compatíveis.

Atualizações suportadas do controlador IP MetroCluster usando os comandos "System controller replace"

Consulte a tabela em "Atualizar controladores em uma configuração IP MetroCluster de quatro nós usando switchover e switchback com comandos "System controller replace" (ONTAP 9.13,1 e posterior)" para obter as plataformas suportadas.

Todas as outras atualizações suportadas do controlador IP MetroCluster

Encontre sua plataforma **Source** nas tabelas de atualização do controlador MetroCluster nesta seção. Se a interseção da linha da plataforma **Source** e da coluna da plataforma **Target** estiver em branco, a atualização não será suportada.

- Se a sua plataforma não estiver listada, não há combinação de atualização de controladora suportada.
- Quando você executa uma atualização de controlador, o tipo de plataforma **deve** antigo e novo corresponde:
  - Você pode atualizar um sistema FAS para um sistema FAS ou um AFF A-Series para um AFF A-Series.
  - Não é possível atualizar um sistema FAS para um AFF A-Series ou um AFF A-Series para um AFF C-Series.

    Por exemplo, se a plataforma que você deseja atualizar for um FAS8200, você pode fazer upgrade para um FAS9000. Não é possível atualizar um sistema FAS8200 para um sistema AFF A700.
- Todos os nós (antigos e novos) na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.

Atualizações suportadas do controlador IP AFF e FAS MetroCluster

A tabela a seguir mostra as combinações de plataforma suportadas para atualizar um sistema AFF ou FAS manualmente em uma configuração IP MetroCluster:

FAS and AFF		Target MetroCluster IP platform												
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150													
	FAS2750 AFF A220													
	FAS500f AFF C250 AFF A250													
	FAS8200 AFF A300									Note 3		Note 2	Note 3	
	AFF A320													
	FAS8300 AFF C400 AFF A400									Note 3		Note 2	Note 3	
	FAS8700											Note 2		
	FAS9000 AFF A700									Note 3		Note 1	Note 3	
	AFF A70													
	AFF C800 AFF A800												Note 4	
	FAS9500 AFF A900												Note 3	
	AFF A90													
	AFF A1K													

- Nota 1: Para esta atualização, utilize o procedimento "Atualizar controladores de AFF A700/FAS9000 para AFF A900/FAS9500 em uma configuração IP MetroCluster usando switchover e switchback (ONTAP 9.10,1 ou posterior)"
- Observação 2: Atualizações de controladora são suportadas em sistemas que executam o ONTAP 9.13,1 ou posterior.
- Nota 3: A plataforma de destino não pode ter unidades internas até que a atualização da controladora esteja concluída. Você pode adicionar as unidades internas após a atualização.
- Nota 4: Requer a substituição dos módulos do controlador.

Atualizações suportadas do controlador IP ASA MetroCluster

A tabela a seguir mostra as combinações de plataforma suportadas para atualizar um sistema ASA manualmente em uma configuração IP do MetroCluster:

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								Note 1
	ASA C800								
	ASA A800								
	ASA A900								

- Observação 1: Atualizações de controladora são suportadas em sistemas que executam o ONTAP 9.13,1 ou posterior.

Atualizações de controladora MetroCluster FC compatíveis

Encontre sua plataforma **Source** nas tabelas de atualização do controlador MetroCluster nesta seção. Se a interseção da linha da plataforma **Source** e da coluna da plataforma **Target** estiver em branco, a atualização não será suportada.

- Se a sua plataforma não estiver listada, não há combinação de atualização de controladora suportada.
- Quando você executa uma atualização de controlador, o tipo de plataforma **deve** antigo e novo corresponde:
  - Você pode atualizar um sistema FAS para um sistema FAS ou um AFF A-Series para um AFF A-

Series.

- Não é possível atualizar um sistema FAS para um AFF A-Series ou um AFF A-Series para um AFF C-Series.

  Por exemplo, se a plataforma que você deseja atualizar for um FAS8200, você pode fazer upgrade para um FAS9000. Não é possível atualizar um sistema FAS8200 para um sistema AFF A700.

- Todos os nós (antigos e novos) na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.

Atualizações compatíveis de controladora AFF e FAS MetroCluster FC

A tabela a seguir mostra as combinações de plataforma compatíveis para atualizar um sistema AFF ou FAS em uma configuração MetroCluster FC:

FAS and AFF		Target MetroCluster FC platform									
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1		Note 1			
	AFF8020		Note 1		Note 1		Note 1		Note 1		
	FAS8040 FAS8060 FAS8080										
	AFF8040 AFF8060 AFF8080										
	FAS8200					Note 2		Note 2		Note 4	
	AFF A300						Note 2		Note 2		Note 4
	FAS8300									Note 4	
	AFF A400										Note 4
	FAS9000									Note 3	
	AFF A700										Note 3
	FAS9500										
	AFF A900										

- Observação 1: Para atualizar controladores quando as conexões FCVI em nós FAS8020 ou AFF8020 existentes usam as portas 1c e 1D, consulte o seguinte "artigo da base de conhecimento".
- Observação 2: Atualizações de controladora de plataformas AFF A300 ou FAS8200 usando as portas integradas 0e e 0f como conexões FC-VI só são compatíveis com os seguintes sistemas:
  - ONTAP 9.9,1 e anteriores
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1GA
  - ONTAP 9.13,1 e posterior

  Para obter mais informações, consulte o "Relatório público".

- Nota 3: Para esta atualização, consulte "Atualizar controladores de AFF A700/FAS9000 para AFF A900/FAS9500 em uma configuração MetroCluster FC usando switchover e switchback (ONTAP 9.10,1 ou posterior)"
- Observação 4: Atualizações de controladora são suportadas em sistemas que executam o ONTAP 9.13,1 ou posterior.

Atualizações de controladora ASA MetroCluster FC compatíveis

A tabela a seguir mostra as combinações de plataforma compatíveis para atualizar um sistema ASA em uma configuração MetroCluster FC:

Fonte da plataforma MetroCluster FC	Plataforma FC MetroCluster de destino	Suportado?
ASA A400	ASA A400	Sim
	ASA A900	Não
ASA A900	ASA A400	Não
	ASA A900	Sim (consulte a Nota 1)

- Observação 1: Atualizações de controladora são suportadas em sistemas que executam o ONTAP 9.14,1 ou posterior.

Escolha um procedimento que use o processo de comutação e switchback

Depois de analisar as combinações de atualização suportadas, escolha o procedimento correto de atualização do controlador para a sua configuração.

Tipo MetroCluster	Método de atualização	Versão de ONTAP	Procedimento
IP	Atualize com os comandos 'stystem controller replace'	9.13.1 e mais tarde	"Ligação ao procedimento"
FC	Atualize com os comandos 'stystem controller replace'	9.10.1 e mais tarde	"Ligação ao procedimento"
FC	Atualização manual com comandos CLI (somente AFF A700/FAS9000 para AFF A900/FAS9500)	9.10.1 e mais tarde	"Ligação ao procedimento"
IP	Atualização manual com comandos CLI (somente AFF A700/FAS9000 para AFF A900/FAS9500)	9.10.1 e mais tarde	"Ligação ao procedimento"
FC	Atualização manual com comandos CLI	9,8 e mais tarde	"Ligação ao procedimento"

IP	Atualização manual com comandos CLI	9,8 e mais tarde	"Ligação ao procedimento"

Escolhendo um procedimento usando realocação agregada

Em um procedimento de atualização de controladora baseado em ARL, as operações de realocação agregada são usadas para mover dados da configuração antiga para a configuração nova e atualizada sem interrupções.

Tipo MetroCluster	Realocação de agregados	Versão de ONTAP	Procedimento
FC	Usando comandos "System controller replace" para atualizar modelos de controladora no mesmo chassi	9.10.1 e mais tarde	"Ligação ao procedimento"
FC	Usando `system controller replace` comandos	9,8 e mais tarde	"Ligação ao procedimento"
FC	Usando `system controller replace` comandos	9,5 a 9,7	"Ligação ao procedimento"
FC	Usando comandos ARL manuais	9,8	"Ligação ao procedimento"
FC	Usando comandos ARL manuais	9,7 e anteriores	"Ligação ao procedimento"

Escolher um método de atualização do sistema

O procedimento de atualização do sistema que você usa depende do modelo da plataforma e do tipo de configuração do MetroCluster. Os procedimentos de atualização se aplicam aos controladores e às gavetas de storage. Nos procedimentos de atualização, novos controladores e compartimentos são adicionados à configuração do MetroCluster, criando um segundo grupo de DR e migrando os dados para os novos nós sem interrupções. Os controladores originais são então desativados.

Combinações de atualização técnica IP MetroCluster suportadas

- Você deve concluir o procedimento de atualização técnica antes de adicionar uma nova carga.
- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do ONTAP. Por exemplo, se você tiver uma configuração de oito nós, todos os oito nós devem estar executando a mesma versão do ONTAP.

- Não exceda quaisquer limites de objeto do "inferior" das plataformas na combinação. Aplique o limite inferior de objetos das duas plataformas.
- Se os limites da plataforma de destino forem inferiores aos limites do MetroCluster, você deverá reconfigurar o MetroCluster para estar nos limites da plataforma de destino ou abaixo antes de adicionar os novos nós.
- Consulte a "Hardware Universe"para obter os limites da plataforma.

Combinações de atualização técnica AFF e FAS MetroCluster IP suportadas

A tabela a seguir mostra as combinações de plataforma suportadas para atualizar um sistema AFF ou FAS em uma configuração IP MetroCluster:

AFF and FAS		Target MetroCluster IP platform												
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150	Note 1	Note 1	Note 1			Note 1	Note 1	Note 1		Note 1	Note 1		
	FAS2750 AFF A220	Note 1	Note 1	Note 1			Note 1	Note 1	Note 1		Note 1	Note 1		
	FAS500f AFF C250 AFF A250	Note 1	Note 1	Note 1			Note 1	Note 1	Note 1		Note 1	Note 1		
	FAS8200 AFF A300													
	AFF A320													
	FAS8300 AFF C400 AFF A400													
	FAS8700													
	FAS9000 AFF A700													
	AFF A70													
	AFF C800 AFF A800													
	FAS9500 AFF A900													
	AFF A90													
	AFF A1K													

Nota 1: esta combinação requer ONTAP 9.13,1 ou posterior.

Combinações de atualização técnica IP ASA MetroCluster suportadas

A tabela a seguir mostra as combinações de plataforma suportadas para atualizar um sistema ASA em uma configuração IP do MetroCluster:

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

Combinações de atualização técnica do MetroCluster FC compatíveis

- Você deve concluir o procedimento de atualização técnica antes de adicionar uma nova carga.
- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do ONTAP. Por exemplo, se você tiver uma configuração de oito nós, todos os oito nós devem estar executando a mesma versão do ONTAP.
- Não exceda quaisquer limites de objeto do "inferior" das plataformas na combinação. Aplique o limite inferior de objetos das duas plataformas.

- Se os limites da plataforma de destino forem inferiores aos limites do MetroCluster, você deverá reconfigurar o MetroCluster para estar nos limites da plataforma de destino ou inferiores antes de adicionar os novos nós.
- Consulte a "Hardware Universe"para obter os limites da plataforma.

Combinações de atualização técnica compatíveis com AFF e FAS MetroCluster FC

A tabela a seguir mostra as combinações de plataforma compatíveis para atualizar um sistema AFF ou FAS em uma configuração MetroCluster FC:

FAS and AFF		Destination MetroCluster FC platform							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8200	■	■	■	■	■	■	■	■
	AFF A300	■	■	■	■	■	■	■	■
	FAS8300			■	■	■	■	■	■
	AFF A400			■	■	■	■	■	■
	FAS9000					■	■	■	■
	AFF A700					■	■	■	■
	FAS9500							■	■
	AFF A900							■	■

Combinações de atualização técnica do ASA MetroCluster FC compatíveis

A tabela a seguir mostra as combinações de plataforma compatíveis para atualizar um sistema ASA em uma configuração MetroCluster FC:

Fonte da plataforma MetroCluster FC	Plataforma FC MetroCluster de destino	Suportado?
ASA A400	ASA A400	Sim
	ASA A900	Não
ASA A900	ASA A400	Não
	ASA A900	Sim

Escolha um procedimento de atualização

Escolha o procedimento de atualização para sua configuração na tabela a seguir:

Atualizar método	Tipo de configuração	Versão de ONTAP	Procedimento
• Método: Expanda a configuração do MetroCluster e remova os nós antigos	FC de quatro nós	9,6 e mais tarde	"Ligação ao procedimento"
• Método: Expanda a configuração do MetroCluster e remova os nós antigos	IP de quatro nós	9,8 e mais tarde	"Ligação ao procedimento"

Escolha um procedimento de expansão

O procedimento de expansão usado depende do tipo de configuração do MetroCluster e da versão do ONTAP.

Um procedimento de expansão envolve a adição de novos controladores e armazenamento à configuração do MetroCluster. A expansão deve manter um número par de controladores em cada local e o procedimento usado depende do número de nós na configuração original do MetroCluster.

Método de expansão	Tipo de configuração	Versão de ONTAP	Procedimento
Método: Expanda um MetroCluster FC de dois nós para quatro	FC de dois nós	ONTAP 9 e posterior (as plataformas devem ser suportadas no ONTAP 9 .2 e posterior)	"Ligação ao procedimento"
Método: Expanda um MetroCluster FC de quatro nós para oito	FC de quatro nós	ONTAP 9 ou posterior	"Ligação ao procedimento"
Método: Expanda um IP MetroCluster de quatro nós para oito	IP de quatro nós	ONTAP 9.9,1 e posterior	"Ligação ao procedimento"

Atualizar controladores em uma configuração IP MetroCluster de quatro nós usando switchover e switchback com comandos "System controller replace" (ONTAP 9.13,1 e posterior)

Você pode usar essa operação de switchover automatizado guiado por MetroCluster para executar uma atualização sem interrupções do controlador em uma configuração de IP MetroCluster de quatro nós. Outros componentes (como prateleiras de armazenamento ou switches) não podem ser atualizados como parte deste procedimento.

Atualizações suportadas do controlador IP MetroCluster usando os comandos "System controller replace"

Encontre sua plataforma **Source** nas tabelas de atualização do controlador MetroCluster nesta seção. Se a interseção da linha da plataforma **Source** e da coluna da plataforma **Target** estiver em branco, a atualização não será suportada.

Antes de iniciar a atualização, reveja as seguintes considerações para verificar se a sua configuração é suportada.

- Se a sua plataforma não estiver listada, não há combinação de atualização de controladora suportada.
- Quando você executa uma atualização de controlador, o tipo de plataforma **deve** antigo e novo corresponde:
  - Você pode atualizar um sistema FAS para um sistema FAS ou um AFF A-Series para um AFF A-Series.
  - Não é possível atualizar um sistema FAS para um AFF A-Series ou um AFF A-Series para um AFF C-Series.

    Por exemplo, se a plataforma que você deseja atualizar for um FAS8200, você pode fazer upgrade para um FAS9000. Não é possível atualizar um sistema FAS8200 para um sistema AFF A700.
- Todos os nós (antigos e novos) na configuração do MetroCluster devem estar executando a mesma versão do ONTAP.

Atualizações suportadas do controlador IP AFF e FAS MetroCluster

A tabela a seguir mostra as combinações de plataforma suportadas para atualizar um sistema AFF ou FAS em uma configuração IP MetroCluster usando comandos "System controller replace":

FAS and AFF		Target MetroCluster IP platform												
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150													
	FAS2750 AFF A220													
	FAS500f AFF C250 AFF A250													
	FAS8200 AFF A300									Note 2		Note 1	Note 2	
	AFF A320													
	FAS8300 AFF C400 AFF A400									Note 2			Note 2	
	FAS8700													
	FAS9000 AFF A700									Note 2			Note 2	
	AFF A70													
	AFF C800 AFF A800												Note 3	
	FAS9500 AFF A900												Note 2	
	AFF A90													
	AFF A1K													

- Observação 1: Atualizações de controladora são suportadas em sistemas que executam o ONTAP 9.13,1 ou posterior.
- Nota 2: A plataforma de destino não pode ter unidades internas até que a atualização da controladora esteja concluída. Você pode adicionar as unidades internas após a atualização.
- Nota 3: Requer a substituição dos módulos do controlador.

Atualizações suportadas do controlador IP ASA MetroCluster

A atualização de controladores usando `system controller replace` comandos em sistemas ASA não é suportada.

"Escolher um método de atualização ou atualização"Consulte para obter mais procedimentos.

Sobre esta tarefa

- Você pode usar este procedimento apenas para atualização do controlador.

  Outros componentes na configuração, como compartimentos de armazenamento ou switches, não podem

ser atualizados ao mesmo tempo.

- Os switches IP MetroCluster (tipo de switch, fornecedor e modelo) e a versão de firmware devem ser suportados nos controladores existentes e novos na configuração de atualização.

  Consulte a "NetApp Hardware Universe"ou a "IMT" para obter informações sobre switches e versões de firmware compatíveis.

- Os sistemas MetroCluster devem estar executando a mesma versão do ONTAP em ambos os sites.
- Você pode usar este procedimento para atualizar controladores em uma configuração IP MetroCluster de quatro nós usando o switchover automatizado baseado em NSO e o switchback.

  > A realização de uma atualização usando ARL (Aggregate relocation) com comandos "Systems controller replace" não é suportada para uma configuração IP MetroCluster de quatro nós.

- Se estiver ativado no seu sistema, "desative a criptografia de ponta a ponta" antes de executar a atualização.
- Você deve usar o procedimento automatizado de atualização do controlador NSO para atualizar os controladores em ambos os locais em sequência.
- Esse procedimento automatizado de atualização de controladora baseada em NSO oferece a capacidade de iniciar a substituição da controladora para um local de recuperação de desastres (DR) da MetroCluster. Você só pode iniciar uma substituição de controlador em um local de cada vez.
- Para iniciar uma substituição de controladora no local A, você precisa executar o comando de inicialização de substituição de controladora a partir do local B. a operação orienta você a substituir os controladores de ambos os nós apenas no local A. Para substituir os controladores no local B, é necessário executar o comando de inicialização de substituição do controlador do local A. Uma mensagem é exibida identificando o local no qual os controladores estão sendo substituídos.

Os seguintes nomes de exemplo são usados neste procedimento:

- Local_A
  - Antes da atualização:
    - Node_A_1-old
    - Node_A_2-old
  - Após a atualização:
    - Node_A_1-novo
    - Node_A_2-novo
- Local_B
  - Antes da atualização:
    - Node_B_1-old
    - Node_B_2-old
  - Após a atualização:
    - Node_B_1-novo
    - Node_B_2-novo

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Defina o bootarg necessário no sistema existente

Se você estiver atualizando para um sistema AFF A70, AFF A90 ou AFF A1K, siga as etapas para definir o `hw.cxgbe.toe_keepalive_disable=1` bootarg.

> Se você estiver atualizando para um sistema AFF A70, AFF A90 ou AFF A1K, **deve** concluir esta tarefa antes de executar a atualização. Esta tarefa **somente** se aplica a atualizações para um sistema AFF A70, AFF A90 ou AFF A1K a partir de um sistema suportado. Para todas as outras atualizações, você pode pular esta tarefa e ir diretamente para Prepare-se para a atualização.

Passos

1. Pare um nó em cada local e permita que seu parceiro de HA faça um takeover do nó:

   ```
   halt -node <node_name>
   ```

2. No `LOADER` prompt do nó interrompido, digite o seguinte:

   ```
   setenv hw.cxgbe.toe_keepalive_disable 1

   saveenv

   printenv hw.cxgbe.toe_keepalive_disable
   ```

3. Inicialize o nó:

   ```
   boot_ontap
   ```

4. Quando o nó for inicializado, execute um giveback para o nó no prompt:

   ```
   storage failover giveback -ofnode <node_name>
   ```

5. Repita as etapas em cada nó no grupo DR que está sendo atualizado.

Prepare-se para a atualização

Para se preparar para a atualização da controladora, é necessário realizar pré-verificações do sistema e coletar as informações de configuração.

Antes de iniciar as pré-verificações, se o Mediador ONTAP estiver instalado, ele será automaticamente detetado e removido. Para confirmar a remoção, você será solicitado a digitar um nome de usuário e senha. Ao concluir a atualização, ou se as pré-verificações falharem ou optar por não prosseguir com a atualização, é Reconfigure manualmente o Mediador ONTAPnecessário .

Em qualquer estágio durante a atualização, você pode executar o `system controller replace show` comando ou `system controller replace show-details` do site A para verificar o status. Se os comandos devolverem uma saída em branco, aguarde alguns minutos e execute novamente o comando.

Passos

1. Inicie o procedimento de substituição automática do controlador A partir do local A para substituir os controladores no local B:

   ```
   system controller replace start -nso true
   ```

   A operação automatizada executa as pré-verificações. Se não forem encontrados problemas, a operação será interrompida para que você possa coletar manualmente as informações relacionadas à configuração.

- Se você não executar o `system controller replace start -nso true` comando, o procedimento de atualização do controlador escolhe o switchover automatizado baseado em NSO e o switchback como o procedimento padrão em sistemas IP MetroCluster.
- O sistema de origem atual e todos os sistemas de destino compatíveis são apresentados. Se você substituiu o controlador de origem por um controlador que tenha uma versão diferente do ONTAP ou uma plataforma não compatível, a operação de automação pára e relata um erro após os novos nós serem inicializados. Para voltar a colocar o cluster num estado saudável, tem de seguir o procedimento de recuperação manual.

  O `system controller replace start` comando pode relatar o seguinte erro de pré-verificação:

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- --------------
------------------------------------
Node-A-1    Failed         MetroCluster check failed.
Reason : MCC check showed errors in component aggregates
```

  Verifique se esse erro ocorreu porque você tem agregados sem espelhamento ou devido a outro problema agregado. Verifique se todos os agregados espelhados estão saudáveis e não degradados ou degradados por espelho. Se esse erro for devido apenas a agregados sem espelhamento, você pode substituir esse erro selecionando a `-skip-metrocluster-check true` opção no `system controller replace start` comando. Se o storage remoto estiver acessível, os agregados sem espelhamento estarão online após o switchover. Se o link de storage remoto falhar, os agregados sem espelhamento não estarão online.

2. Colete manualmente as informações de configuração fazendo login no local B e seguindo os comandos listados na mensagem do console sob o `system controller replace show` comando ou `system controller replace show-details`.

Reúna informações antes da atualização

Antes de atualizar, se o volume raiz estiver criptografado, você deverá reunir a chave de backup e outras informações para inicializar os novos controladores com os antigos volumes de raiz criptografados.

Sobre esta tarefa

Esta tarefa é executada na configuração IP do MetroCluster existente.

Passos

1. Identifique os cabos dos controladores existentes para que possa identificar facilmente os cabos ao configurar os novos controladores.
2. Exiba os comandos para capturar a chave de backup e outras informações:

   `system controller replace show`

Execute os comandos listados sob o `show` comando do cluster de parceiros.

O `show` comando output exibe três tabelas contendo os IPs de interface MetroCluster, IDs de sistema e UUIDs de sistema. Esta informação é necessária mais tarde no procedimento para definir os bootargs quando você inicializar o novo nó.

3. Reúna as IDs do sistema dos nós na configuração do MetroCluster:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Durante o procedimento de atualização, você substituirá esses IDs de sistema antigos pelos IDs de sistema dos novos módulos de controladora.

   Neste exemplo para uma configuração IP MetroCluster de quatro nós, os seguintes IDs de sistema antigos são recuperados:

   - Node_A_1-old: 4068741258
   - Node_A_2-old: 4068741260
   - Node_B_1-old: 4068741254
   - Node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        --------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

   Neste exemplo para uma configuração IP MetroCluster de dois nós, os seguintes IDs de sistema antigos são recuperados:

   - Node_A_1: 4068741258
   - Nó_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Reúna informações de porta e LIF para cada nó antigo.

   Você deve reunir a saída dos seguintes comandos para cada nó:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node <node-name> -type physical`
   - `network port vlan show -node <node-name>`
   - `network port ifgrp show -node <node-name> -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node <node-name> sysconfig -a`
   - `aggr show -r`
   - `disk show`
   - `system node run <node-name> disk show`
   - `vol show -fields type`
   - `vol show -fields type , space-guarantee`
   - `vserver fcp initiator show`
   - `storage disk show`
   - `metrocluster configuration-settings interface show`

5. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves:

   `security key-manager backup show`

7. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações sobre as chaves e senhas.

   Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

   a. Se o Gerenciador de chaves integrado estiver configurado:

      `security key-manager onboard show-backup`

      Você precisará da senha mais tarde no procedimento de atualização.

   b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

      `security key-manager external show -instance`

   `security key-manager key query`

8. Depois de concluir a recolha das informações de configuração, retome a operação:

   `system controller replace resume`

Remova a configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, o ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes de substituir a controladora antiga.

Passos

1. "Remova a configuração existente do MetroCluster" Do software tiebreaker.
2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Substitua os controladores antigos e inicialize os novos controladores

Depois de reunir informações e retomar a operação, a automação prossegue com a operação de comutação.

Sobre esta tarefa

A operação de automação inicia as operações de comutação. Depois que essas operações forem concluídas, a operação será interrompida em **pausado para intervenção do usuário** para que você possa montar e instalar os controladores, inicializar os controladores do parceiro e reatribuir os discos agregados raiz ao novo módulo do controlador a partir do backup flash usando o `sysids` coletado anteriormente.

Antes de começar

Antes de iniciar o switchover, a operação de automação é interrompida para que você possa verificar

manualmente se todos os LIFs estão "up" no local B. se necessário, traga quaisquer LIFs que são "próprios" para "'up" e retome a operação de automação usando o `system controller replace resume` comando.

Prepare a configuração de rede dos controladores antigos

Para permitir que a rede seja retomada de forma limpa nos novos controladores, verifique se o posicionamento de LIF está correto e remova a configuração de rede dos controladores antigos.

Sobre esta tarefa

- Esta tarefa deve ser executada em cada um dos nós antigos.
- Você usará as informações coletadas em Prepare-se para a atualização.

Passos

1. Inicialize os nós antigos e faça login nos nós:

   ```
   boot_ontap
   ```

2. Modifique as LIFs entre clusters nos controladores antigos para usar uma porta inicial diferente das portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nos novos controladores.

   Esta etapa é necessária para uma atualização bem-sucedida.

   As LIFs entre clusters nos controladores antigos devem usar uma porta inicial diferente das portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nos novos controladores. Por exemplo, quando você faz upgrade para controladoras AFF A90, as portas de interconexão de HA são e1a e e7a e as portas de interconexão de DR IP MetroCluster são E2B e e3b. Você deve mover as LIFs entre clusters nos controladores antigos se eles estiverem hospedados nas portas e1a, e7a, E2B ou e3b.

   Para a distribuição e alocação de portas nos novos nós, consulte o "NetApp Hardware Universe".

   a. Nos controladores antigos, veja os LIFs entre clusters:

      ```
      network interface show -role intercluster
      ```

      Execute uma das ações a seguir, dependendo se as LIFs entre clusters nos controladores antigos usam as mesmas portas que as portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nas novas controladoras.

Se os LIFs entre clusters…	Ir para…
Use a mesma porta inicial	Subpasso b
Utilize uma porta inicial diferente	Passo 3

   b. modifique os LIFs entre clusters para usar uma porta inicial diferente:

      ```
      network interface modify -vserver <vserver> -lif <intercluster_lif> -home
      -port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-
      nodes>
      ```

   c. Verifique se todas as LIFs entre clusters estão em suas novas portas residenciais:

      ```
      network interface show -role intercluster -is-home false
      ```

A saída do comando deve estar vazia, indicando que todas as LIFs entre clusters estão em suas respetivas portas residenciais.

d. Se houver LIFs que não estejam em suas portas residenciais, reverta-os usando o seguinte comando:

```
network interface revert -lif <intercluster_lif>
```

Repita o comando para cada LIF entre clusters que não está na porta inicial.

3. atribua a porta inicial de todos os LIFs de dados no controlador antigo a uma porta comum que é a mesma nos módulos de controladora antigos e novos.

> Se os controladores antigos e novos não tiverem uma porta comum, não será necessário modificar as LIFs de dados. Pule esta etapa e vá diretamente para Passo 4.

a. Apresentar os LIFs:

```
network interface show
```

Todos os dados LIFS, incluindo SAN e nas, serão administradores e operacionais "próprios", uma vez que eles estão ativos no local de comutação (cluster_A).

b. Revise a saída para encontrar uma porta de rede física comum que seja a mesma nos controladores antigos e novos que não seja usada como uma porta de cluster.

Por exemplo, "'e0d'" é uma porta física em controladores antigos e também está presente em novos controladores. "e0d" não é usado como uma porta de cluster ou de outra forma nos novos controladores.

Para obter informações sobre a utilização de portas para modelos de plataforma, consulte a. "NetApp Hardware Universe"

c. Modifique todos os dados LIFS para usar a porta comum como a porta inicial:

```
network interface modify -vserver <svm-name> -lif <data-lif> -home-port
<port-id>
```

No exemplo a seguir, isso é ""e0d"".

Por exemplo:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

4. Modificar domínios de broadcast para remover a VLAN e as portas físicas que precisam ser excluídas:

```
broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name>-ports
<node-name:port-id>
```

Repita esta etapa para todas as portas VLAN e físicas.

5. Remova quaisquer portas VLAN usando portas de cluster como portas membros e grupos de interfaces usando portas de cluster como portas membros.

a. Eliminar portas VLAN:

```
network port vlan delete -node <node-name> -vlan-name <portid-vlandid>
```

Por exemplo:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remover portas físicas dos grupos de interface:

```
network port ifgrp remove-port -node <node-name> -ifgrp <interface-group-name> -port <portid>
```

Por exemplo:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Remova as portas VLAN e grupo de interfaces do domínio de broadcast:

```
network port broadcast-domain remove-ports -ipspace <ipspace> -broadcast -domain <broadcast-domain-name>-ports <nodename:portname,nodename:portname>,..
```

b. Modifique as portas do grupo de interfaces para usar outras portas físicas como membro, conforme necessário.:

```
ifgrp add-port -node <node-name> -ifgrp <interface-group-name> -port <port-id>
```

6. Parar os nós:

```
halt -inhibit-takeover true -node <node-name>
```

Esta etapa deve ser executada em ambos os nós.

7. Verifique se os nós estão no `LOADER` prompt e colete e preserve as variáveis de ambiente atuais.
8. Reúna os valores do bootarg:

```
printenv
```

9. Desligue os nós e as gavetas no local em que a controladora está sendo atualizada.

Configure os novos controladores

É necessário colocar em rack e cabo as novas controladoras.

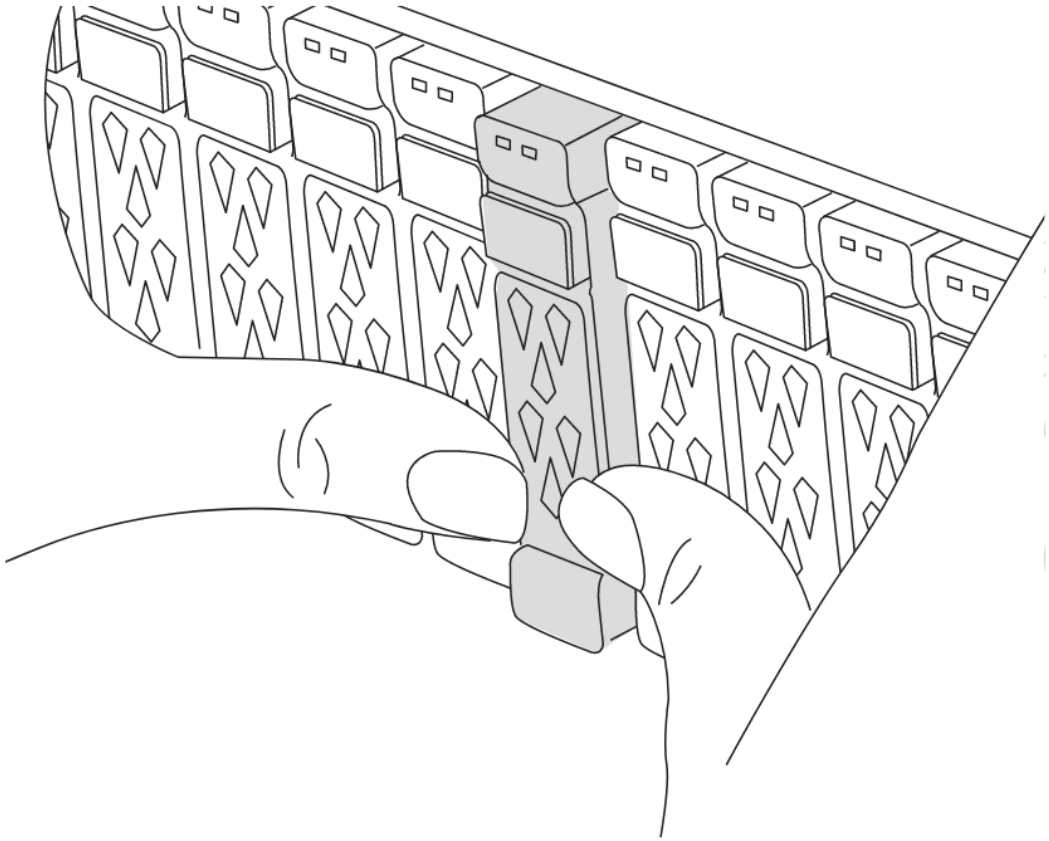
Passos

1. Planeje o posicionamento dos novos módulos de controladora e compartimentos de armazenamento conforme necessário.

O espaço em rack depende do modelo de plataforma dos módulos de controladora, dos tipos de switch e do número de compartimentos de storage em sua configuração.

2. Aterre-se corretamente.
3. Se a atualização exigir a substituição dos módulos da controladora, por exemplo, a atualização de um sistema AFF 800 para um sistema AFF A90, você deve remover o módulo da controladora do chassi quando substituir o módulo da controladora. Para todas as outras atualizações, vá para Passo 4.

   Na parte frontal do chassis, utilize os polegares para empurrar firmemente cada unidade até sentir um batente positivo. Isto confirma que as unidades estão firmemente assentadas contra o plano médio do chassis.



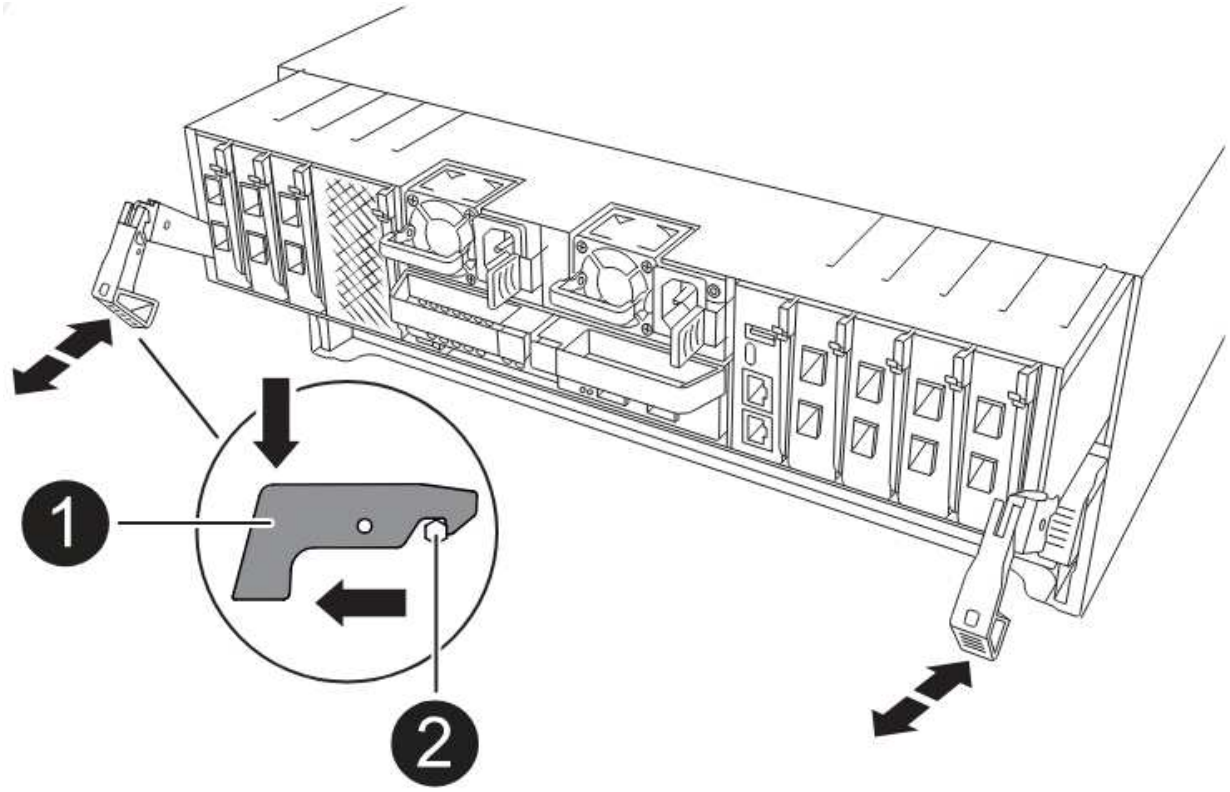
4. instale os módulos do controlador.

   As etapas de instalação que você seguir dependem se a atualização requer a substituição dos módulos da controladora, como uma atualização de um sistema AFF 800 para um sistema AFF A90.

Atualizações que exigem substituição do módulo do controlador

A instalação dos novos controladores separadamente não se aplica a atualizações de sistemas integrados com discos e controladores no mesmo chassi, por exemplo, de um sistema AFF A800 para um sistema AFF A90. Os novos módulos do controlador e as placas de e/S devem ser trocados após desligar os controladores antigos, como mostrado na imagem abaixo.

A imagem de exemplo a seguir é apenas para representação, os módulos do controlador e as placas de e/S podem variar entre sistemas.



Todas as outras atualizações

Instale os módulos do controlador no rack ou gabinete.

5. Faça o cabeamento das conexões de alimentação, console serial e gerenciamento dos controladores, conforme descrito em "Cabeamento dos switches IP MetroCluster"

   Não conete nenhum outro cabo que tenha sido desconetado dos controladores antigos neste momento.

   "Documentação dos sistemas de hardware da ONTAP"

6. Ligue os novos nós e pressione Ctrl-C quando solicitado a exibir o `LOADER` prompt.

Netboot os novos controladores

Depois de instalar os novos nós, você precisa netboot para garantir que os novos nós estejam executando a mesma versão do ONTAP que os nós originais. O termo netboot significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para netboot, você deve colocar uma cópia da imagem de inicialização do ONTAP 9 em um servidor da Web que o sistema possa acessar.

Esta tarefa é executada em cada um dos novos módulos do controlador.

Passos

1. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.
2. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o ficheiro ONTAP-version_image.tgz num diretório acessível à Web.
3. Vá para o diretório acessível pela Web e verifique se os arquivos que você precisa estão disponíveis.

   Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel: ONTAP-version_image.tgz

   Você não precisa extrair o arquivo ONTAP-version_image.tgz.

4. `LOADER`No prompt, configure a conexão netboot para um LIF de gerenciamento:
   - Se o endereçamento IP for DHCP, configure a conexão automática:

     ```
     ifconfig e0M -auto
     ```

   - Se o endereçamento IP for estático, configure a conexão manual:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Execute o netboot.

   ```
   netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
   ```

6. No menu de arranque, selecione a opção **(7) Instalar primeiro o novo software** para transferir e instalar a nova imagem de software no dispositivo de arranque.

   ```
    Disregard the following message: "This procedure is not supported for Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive upgrades of software, not to upgrades of controllers.
   . Se você for solicitado a continuar o procedimento, digite `y` e, quando solicitado a fornecer o pacote, digite o URL do arquivo de imagem: `\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Certifique-se de entrar `n` para ignorar a recuperação de backup quando você vir um prompt semelhante ao seguinte:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Reinicie entrando `y` quando você vir um prompt semelhante ao seguinte:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

Limpe a configuração de um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   `halt`

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

   `set-defaults`

3. Salvar o ambiente:

   `saveenv`

4. No prompt DO Loader, inicie o menu de inicialização:

   `boot_ontap menu`

5. No prompt do menu de inicialização, desmarque a configuração:

   `wipeconfig`

   Responda `yes` ao prompt de confirmação.

   O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

   Responda `yes` ao prompt de confirmação.

Restaure a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:

   a. Verifique as definições atuais das portas: `ucadmin show`

   b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…

CNA FC	`ucadmin modify -m fc -t initiator <adapter-name>`
CNA Ethernet	`ucadmin modify -mode cna <adapter-name>`
Destino de FC	`fcadmin config -t target <adapter-name>`
Iniciador FC	`fcadmin config -t initiator <adapter-name>`

2. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no `LOADER` prompt.

3. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

4. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Defina o estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado HA para todos os componentes deve ser `mccip`.

2. Se o estado do sistema apresentado do controlador ou do chassis não estiver correto, defina o estado HA:

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

3. Verifique e modifique as portas Ethernet conetadas a gavetas NS224 ou switches de storage.

   a. Verifique as portas Ethernet conetadas a gavetas NS224 ou switches de armazenamento:

      `storage port show`

   b. Defina todas as portas Ethernet conetadas a gavetas Ethernet ou switches de armazenamento, incluindo switches compartilhados para armazenamento e cluster, para o `storage` modo:

      `storage port modify -p <port> -m storage`

      Exemplo:

      ```
      *> storage port modify -p e5b -m storage
      Changing NVMe-oF port e5b to storage mode
      ```

      > Isso deve ser definido em todas as portas afetadas para uma atualização bem-sucedida.

      Os discos das gavetas conetadas às portas Ethernet são reportados `sysconfig -v` na saída.

   Consulte a "NetApp Hardware Universe" para obter informações sobre as portas de armazenamento para o sistema para o qual está a atualizar.

   a. Verifique se `storage` o modo está definido e confirme se as portas estão no estado online:

      `storage port show`

4. Parar o nó: `halt`

   O nó deve parar no `LOADER>` prompt.

5. Em cada nó, verifique a data, a hora e o fuso horário do sistema: `show date`
6. Se necessário, defina a data em UTC ou GMT: `set date <mm/dd/yyyy>`
7. Verifique a hora usando o seguinte comando no prompt do ambiente de inicialização: `show time`
8. Se necessário, defina a hora em UTC ou GMT: `set time <hh:mm:ss>`
9. Guarde as definições: `saveenv`
10. Reunir variáveis de ambiente: `printenv`

Atualize os arquivos RCF do switch para acomodar as novas plataformas

Você deve atualizar os switches para uma configuração que suporte os novos modelos de plataforma.

Sobre esta tarefa

Você executa essa tarefa no site que contém os controladores que estão sendo atualizados no momento. Nos exemplos mostrados neste procedimento, estamos atualizando site_B primeiro.

Os switches no site_A serão atualizados quando os controladores no site_A forem atualizados.

Passos

1. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"

2. Baixe e instale os arquivos RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Baixe e instale os arquivos Broadcom RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

Defina as variáveis MetroCluster IP bootarg

Certos valores de inicialização IP do MetroCluster devem ser configurados nos novos módulos do controlador. Os valores devem corresponder aos configurados nos módulos do controlador antigos.

Sobre esta tarefa

- Você precisa dos UUIDs e IDs de sistema identificados anteriormente no procedimento de atualização no Reúna informações antes da atualização.
- Dependendo do modelo da plataforma, você pode especificar o ID da VLAN usando o `-vlan-id` parâmetro. As seguintes plataformas não suportam o `-vlan-id` parâmetro:
  - FAS8200 e AFF A300
  - AFF A320
  - FAS9000 e AFF A700
  - AFF C800, ASA C800, AFF A800 e ASA A800

    Todas as outras plataformas suportam o `-vlan-id` parâmetro.

- Os valores de bootarg do MetroCluster definidos dependem se o novo sistema utiliza portas de cluster/HA partilhadas ou portas MetroCluster/HA partilhadas.

  Os sistemas listados na tabela a seguir usam **portas MetroCluster/HA compartilhadas**.

  Todos os outros sistemas usam **portas de cluster/HA compartilhadas**.

Sistemas AFF e ASA usando portas MetroCluster/HA compartilhadas	Sistemas FAS que usam portas MetroCluster/HA compartilhadas
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

Passos

1. `LOADER>`No prompt, defina os seguintes bootargs nos novos nós no site_B:

   As etapas a seguir dependem das portas usadas pelo novo modelo de plataforma.

Sistemas que usam portas de cluster/HA compartilhadas

a. Defina os seguintes bootargs:

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>
```

> Se as interfaces estiverem usando um ID de VLAN padrão, o `vlan-id` parâmetro não será necessário.

O exemplo a seguir define os valores para node_B_1-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir define os valores para node_B_2-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13,130
```

O exemplo a seguir define os valores para node_B_1-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

O exemplo a seguir define os valores para node_B_2-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13
```

Sistemas que usam portas MetroCluster/HA compartilhadas

a. Defina os seguintes bootargs:

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>
```

> Se as interfaces estiverem usando um ID de VLAN padrão, o `vlan-id` parâmetro não será necessário.

O exemplo a seguir define os valores para node_B_1-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir define os valores para node_B_2-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

O exemplo a seguir define os valores para node_B_1-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

O exemplo a seguir define os valores para node_B_2-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. No prompt dos novos nós `LOADER`, defina os UUIDs:

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

   a. Defina os UUIDs em node_B_1-novo.

      O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_1-novo:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. Defina os UUIDs em node_B_2-novo:

      O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_2-novo:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Determine se os sistemas originais foram configurados para o Advanced Drive Partitioning (ADP) executando o seguinte comando a partir do site que está ativo:

`disk show`

A coluna "container type" (tipo de contentor) apresenta "shared" (partilhado `disk show`) na saída se o ADP estiver configurado. Se o "tipo de contentor" tiver qualquer outro valor, o ADP não está configurado no sistema. A saída de exemplo a seguir mostra um sistema configurado com ADP:

```
::> disk show
                    Usable               Disk    Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner

Info: This cluster has partitioned disks. To get a complete list of
spare disk
      capacity use "storage aggregate show-spare-disks".
----------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

4. Se os sistemas originais foram configurados para ADP, em cada um dos nós de substituição `LOADER`, ative o ADP:

   `setenv bootarg.mcc.adp_enabled true`

5. Defina as seguintes variáveis:

   `setenv bootarg.mcc.local_config_id <original-sys-id>`

   `setenv bootarg.mcc.dr_partner <dr-partner-sys-id>`

   > A `setenv bootarg.mcc.local_config_id` variável deve ser definida como o sys-id do módulo controlador **original**, node_B_1-old.

   a. Defina as variáveis em node_B_1-novo.

      O exemplo a seguir mostra os comandos para definir os valores em node_B_1-novo:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Defina as variáveis em node_B_2-novo.

      O exemplo a seguir mostra os comandos para definir os valores em node_B_2-novo:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Se estiver usando criptografia com gerenciador de chaves externo, defina os bootargs necessários:

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Reatribuir discos agregados de raiz

Reatribua os discos agregados raiz ao novo módulo de controladora, usando o `sysids` recolhido anteriormente

Sobre esta tarefa

Esta tarefa é executada no modo Manutenção.

As IDs de sistema antigas foram identificadas no Reúna informações antes da atualização.

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Nó	ID do sistema antigo	Nova ID do sistema
node_B_1	4068741254	1574774970

Passos

1. Cable todas as outras conexões aos novos módulos de controladora (FC-VI, armazenamento, interconexão de cluster, etc.).
2. Interrompa o sistema e inicie para o modo de manutenção a partir do `LOADER` prompt:

```
boot_ontap maint
```

3. Exiba os discos de propriedade de node_B_1-old:

```
disk show -a
```

A saída do comando mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (4068741254). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

Antes de prosseguir com a reatribuição de disco, você deve verificar se os discos pool0 e pool1 pertencentes ao agregado raiz do nó são exibidos na `disk show` saída. No exemplo a seguir, a saída lista os discos pool0 e pool1 de propriedade do node_B_1-old.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------              -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Reatribua os discos agregados de raiz nas gavetas de unidades à nova controladora:

   `disk reassign -s <old-sysid> -d <new-sysid>`

   > Se o sistema IP do MetroCluster estiver configurado com particionamento de disco avançado, você deverá incluir o ID do sistema do parceiro DR executando o `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid` comando.

   O exemplo a seguir mostra a reatribuição de unidades:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verifique se todos os discos estão reatribuídos conforme esperado:

`disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                     POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------             -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Exibir o status agregado:

   `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Repita as etapas acima no nó do parceiro (node_B_2-novo).

Inicialize os novos controladores

Você deve reiniciar os controladores a partir do menu de inicialização para atualizar a imagem flash do controlador. Etapas adicionais são necessárias se a criptografia estiver configurada.

Você pode reconfigurar VLANs e grupos de interface. Se necessário, modifique manualmente as portas para os LIFs de cluster e os detalhes do domínio de broadcast antes de retomar a operação usando o `system controller replace resume` comando.

Sobre esta tarefa

Esta tarefa deve ser executada em todos os novos controladores.

Passos

1. Parar o nó:

   `halt`

2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

   `setenv bootarg.kmip.init.ipaddr <ip-address>`

   `setenv bootarg.kmip.init.netmask <netmask>`

   `setenv bootarg.kmip.init.gateway <gateway-address>`

   `setenv bootarg.kmip.init.interface <interface-id>`

3. Apresentar o menu de arranque:

   `boot_ontap menu`

4. Se a criptografia raiz for usada, selecione a opção do menu de inicialização para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…

Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

5. No menu de inicialização, execute a opção "'6".

   A opção "'6" reiniciará o nó duas vezes antes de concluir.

   Responda "y" aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

   Durante uma das reinicializações após a opção "'6", o prompt de confirmação `Override system ID? {y|n}` aparece. Introduza `y`.

6. Se a criptografia raiz for usada, selecione a opção do menu de inicialização novamente para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

   Dependendo da configuração do gerenciador de chaves, execute o procedimento de recuperação selecionando a opção ""10"" ou a opção ""11"", seguida da opção ""6"" no primeiro prompt do menu de inicialização. Para inicializar os nós completamente, você pode precisar repetir o procedimento de recuperação continuado pela opção "'1'" (inicialização normal).

7. Inicialize os nós:

```
boot_ontap
```

8. Aguarde que os nós substituídos iniciem.

   Se um dos nós estiver no modo de aquisição, execute um giveback usando o `storage failover giveback` comando.

9. Verifique se todas as portas estão em um domínio de broadcast:

   a. Veja os domínios de broadcast:

      ```
      network port broadcast-domain show
      ```

   b. Se um novo domínio de broadcast for criado para as portas de dados nos controladores recém-atualizados, exclua o domínio de broadcast:

      > Exclua apenas o novo domínio de broadcast. Não exclua nenhum dos domínios de broadcast que existiam antes de iniciar a atualização.

      ```
      broadcast-domain delete -broadcast-domain <broadcast_domain_name>
      ```

   c. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

      "Adicionar ou remover portas de um domínio de broadcast"

   d. Adicione a porta física que hospedará os LIFs entre clusters ao domínio de broadcast correspondente.

   e. Modifique LIFs entre clusters para usar a nova porta física como porta inicial.

   f. Depois que os LIFs entre clusters estiverem ativos, verifique o status de peer do cluster e restabeleça o peering de cluster conforme necessário.

      Talvez seja necessário reconfigurar o peering de cluster.

      "Criando um relacionamento de cluster peer"

   g. Recrie VLANs e grupos de interface conforme necessário.

      A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

      "Criando um VLAN"

   "Combinando portas físicas para criar grupos de interface"

   a. Verifique se o cluster de parceiros está acessível e se a configuração é ressincronizada com êxito no cluster de parceiros:

      ```
      metrocluster switchback -simulate true
      ```

10. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…

Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver <svm-name> -node <node-name> -key-server <host_name`

11. Verifique se o MetroCluster está configurado corretamente. Verifique o status do nó:

    `metrocluster node show`

    Verifique se os novos nós (site_B) estão em **aguardando o estado switchback** do site_A.

Verifique e restaure a configuração do LIF

Verifique se os LIFs estão hospedados em nós apropriados antes de prosseguir com a operação de switchback automatizado.

Sobre esta tarefa

- Esta tarefa é executada no site_B.

> Você deve verificar se o local das LIFs de dados está correto nos novos nós antes de executar um switchback. Quando você alterna a configuração, o ONTAP tenta retomar o tráfego na porta inicial usada pelos LIFs. A falha de e/S pode ocorrer quando a conexão da porta inicial com a porta do switch e VLAN estiver incorreta.

Passos

1. Verifique se os LIFs estão hospedados no nó e portas apropriados antes do switchback.

    a. Mude para o nível de privilégio avançado:

    `set -privilege advanced`

    b. Exiba os LIFs e confirme se cada data LIF está usando a porta inicial correta:

    `network interface show`

    c. Modifique quaisquer LIFs que não estejam usando a porta inicial correta:

    `network interface modify -vserver <svm-name> -lif <data-lif> -home-port <port-id>`

    Se o comando retornar um erro, você pode substituir a configuração da porta:

    `vserver config override -command "network interface modify -vserver <svm-name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node <new_node_name>"`

Ao entrar no comando Network Interface Modify dentro `vserver config override` do comando, não é possível usar o recurso Tab Autocomplete. Você pode criar a rede `interface modify` usando o autocomplete e, em seguida, incorporá-la no `vserver config override` comando.

a. Confirme se todas as LIFs de dados estão agora na porta inicial correta:

```
network interface show
```

b. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

2. Reverter as interfaces para o seu nó inicial:

```
network interface revert * -vserver <svm-name>
```

Execute esta etapa em todas as SVMs, conforme necessário.

3. Retomar a operação:

```
system controller replace resume
```

Conclua a atualização

A operação de automação executa verificações do sistema e, em seguida, pausa para que você possa verificar a acessibilidade da rede. Após a verificação, a fase de recuperação de recursos é iniciada e a operação de automação executa switchback no local A e pausa nas verificações pós-atualização. Depois de retomar a operação de automação, ele executa as verificações de pós-atualização e, se nenhum erro for detetado, marca a atualização como concluída.

Passos

1. Verifique a acessibilidade da rede seguindo a mensagem do console.
2. Após concluir a verificação, retome a operação:

```
system controller replace resume
```

3. A operação de automação executa `heal-aggregate` operações de switchback , `heal-root-aggregate` e no local A e as verificações pós-atualização. Quando a operação for interrompida, verifique manualmente o status do SAN LIF e verifique a configuração da rede seguindo a mensagem do console.
4. Após concluir a verificação, retome a operação:

```
system controller replace resume
```

5. Verifique o status das verificações de pós-atualização:

```
system controller replace show
```

Se as verificações pós-atualização não reportaram erros, a atualização está concluída.

6. Depois de concluir a atualização do controlador, inicie sessão no local B e verifique se os controladores substituídos estão configurados corretamente.

Reconfigure o Mediador ONTAP

Configure manualmente o ONTAP Mediator que foi removido automaticamente antes de iniciar a atualização.

1. Siga as etapas em "Configure o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster".

Restaure o monitoramento do tiebreaker

Se a configuração do MetroCluster tiver sido configurada anteriormente para monitoramento pelo software tiebreaker, você poderá restaurar a conexão tiebreaker.

1. Siga as etapas em "Adição de configurações do MetroCluster".

Configurar criptografia de ponta a ponta

Se for compatível com o sistema, você poderá criptografar o tráfego de back-end, como NVlog e dados de replicação de armazenamento, entre os sites IP do MetroCluster. "Configurar criptografia de ponta a ponta"Consulte para obter mais informações.

Atualização de controladores em uma configuração MetroCluster FC usando switchover e switchback

Você pode usar a operação switchover do MetroCluster para fornecer serviços sem interrupções aos clientes enquanto os módulos de controladora no cluster de parceiros são atualizados. Outros componentes (como prateleiras de armazenamento ou switches) não podem ser atualizados como parte deste procedimento.

Combinações de plataformas suportadas

Você pode atualizar certas plataformas usando a operação de comutação e switchback em uma configuração MetroCluster FC.

Para obter informações sobre quais combinações de atualização de plataforma são suportadas, consulte a tabela de atualização do MetroCluster FC "Escolha um procedimento de atualização da controladora"no .

```
https://docs.netapp.com/us-en/ontap-
metrocluster/upgrade/concept_choosing_an_upgrade_method_mcc.html["Escolher
um método de atualização ou atualização"]Consulte para obter mais
procedimentos.
```

Sobre esta tarefa

- Você pode usar este procedimento apenas para atualização do controlador.

  Outros componentes na configuração, como compartimentos de armazenamento ou switches, não podem ser atualizados ao mesmo tempo.

- Pode utilizar este procedimento com determinadas versões do ONTAP:

- Configurações de dois nós são compatíveis com o ONTAP 9.3 e versões posteriores.
- Configurações de quatro e oito nós são compatíveis com o ONTAP 9.8 e versões posteriores.

  Não use este procedimento em configurações de quatro ou oito nós que executam versões do ONTAP anteriores a 9,8.

- Suas plataformas originais e novas devem ser compatíveis e suportadas.

  "NetApp Hardware Universe"

  Se as plataformas originais ou novas forem sistemas FAS8020 ou AFF8020 usando as portas 1c e 1D no modo FC-VI, consulte o artigo da base de dados de Conhecimento "Atualizando controladores quando as conexões FCVI em nós FAS8020 ou AFF8020 existentes usam as portas 1c e 1D."

- As licenças em ambos os locais devem corresponder. Pode obter novas licenças a partir "Suporte à NetApp"do .
- Esse procedimento se aplica a módulos do controlador em uma configuração do MetroCluster FC (um MetroCluster elástico de dois nós ou uma configuração de MetroCluster conetada à malha de dois, quatro ou oito nós).
- Todas as controladoras no mesmo grupo de DR devem ser atualizadas durante o mesmo período de manutenção.

  A operação da configuração do MetroCluster com diferentes tipos de controladora no mesmo grupo de DR não é suportada fora desta atividade de manutenção. Para configurações de MetroCluster de oito nós, os controladores dentro de um grupo de DR precisam ser os mesmos, mas ambos os grupos de DR podem usar tipos de controlador diferentes.

- Recomenda-se o mapeamento antecipado de conexões Ethernet e FC entre nós originais e novos nós.
- Se a nova plataforma tiver menos slots do que o sistema original, ou se tiver menos ou diferentes tipos de portas, talvez seja necessário adicionar um adaptador ao novo sistema.

  Para obter mais informações, consulte a. "NetApp Hardware Universe"

Os seguintes nomes de exemplo são usados neste procedimento:

- Local_A
  - Antes da atualização:
    - Node_A_1-old
    - Node_A_2-old
  - Após a atualização:
    - Node_A_1-novo
    - Node_A_2-novo
- Local_B
  - Antes da atualização:
    - Node_B_1-old
    - Node_B_2-old

- Após a atualização:
  - Node_B_1-novo
  - Node_B_2-novo

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Preparando-se para a atualização

Antes de fazer quaisquer alterações na configuração do MetroCluster existente, você deve verificar a integridade da configuração, preparar as novas plataformas e executar outras tarefas diversas.

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a atualização.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:

   a. Verifique se os nós são multipathed: Mais
   `node run -node node-name sysconfig -a`

      Você deve emitir este comando para cada nó na configuração do MetroCluster.

   b. Verifique se não há discos quebrados na configuração:

      ```
      storage disk show -broken
      ```

      Você deve emitir este comando em cada nó na configuração do MetroCluster.

   c. Verifique se existem alertas de saúde:

      ```
      system health alert show
      ```

      Você deve emitir este comando em cada cluster.

   d. Verifique as licenças nos clusters:

      ```
      system license show
      ```

Você deve emitir este comando em cada cluster.

e. Verifique os dispositivos conetados aos nós:

```
network device-discovery show
```

Você deve emitir este comando em cada cluster.

f. Verifique se o fuso horário e a hora estão definidos corretamente em ambos os sites:

```
cluster date show
```

Você deve emitir este comando em cada cluster. Pode utilizar os `cluster date` comandos para configurar a hora e o fuso horário.

2. Verifique se existem alertas de estado nos interrutores (se presentes):

```
storage switch show
```

Você deve emitir este comando em cada cluster.

3. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

```
metrocluster show
```

   b. Confirme se todos os nós esperados são mostrados:

```
metrocluster node show
```

   c. Emita o seguinte comando:

```
metrocluster check run
```

   d. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

4. Verifique o cabeamento do MetroCluster com a ferramenta Config Advisor.
   a. Baixe e execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

   b. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Mapeamento de portas dos nós antigos para os novos nós

É necessário Planejar o mapeamento das LIFs em portas físicas nos nós antigos para as portas físicas nos novos nós.

Sobre esta tarefa

Quando o novo nó é inicializado pela primeira vez durante o processo de atualização, ele reproduzirá a

configuração mais recente do nó antigo que está substituindo. Quando você inicializa node_A_1-novo, o ONTAP tenta hospedar LIFs nas mesmas portas que foram usadas no node_A_1-old. Portanto, como parte da atualização, você deve ajustar a configuração de porta e LIF para que seja compatível com a do nó antigo. Durante o procedimento de atualização, você executará etapas nos nós antigos e novos para garantir a configuração correta de cluster, gerenciamento e LIF de dados.

A tabela a seguir mostra exemplos de alterações de configuração relacionadas aos requisitos de porta dos novos nós.

Portas físicas de interconexão de cluster		
Controlador antigo	Novo controlador	Ação necessária
e0a, e0b	e3a, e3b	Nenhuma porta correspondente. Após a atualização, você deve recriar as portas do cluster. "Preparando portas do cluster em um módulo do controlador existente"
e0c, e0d	e0a, e0b, e0c, e0d	e0c e e0d são portas correspondentes. Você não precisa alterar a configuração, mas após a atualização, você pode espalhar suas LIFs de cluster pelas portas de cluster disponíveis.

Passos

1. Determine quais portas físicas estão disponíveis nos novos controladores e quais LIFs podem ser hospedados nas portas.

   O uso da porta do controlador depende do módulo da plataforma e quais switches você usará na configuração IP do MetroCluster. Você pode coletar o uso de portas das novas plataformas do "NetApp Hardware Universe".

   Identifique também a utilização do slot de placa FC-VI.

2. Planeje o uso da porta e, se desejado, preencha as tabelas a seguir para referência para cada um dos novos nós.

   Irá consultar a tabela à medida que realizar o procedimento de atualização.

	Node_A_1-old			Node_A_1-novo		
LIF	Portas	IPspaces	Domínios de broadcast	Portas	IPspaces	Domínios de broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gerenciamento de nós						

Gerenciamento de clusters						
Dados 1						
Dados 2						
Dados 3						
Dados 4						
SAN						
Porta entre clusters						

Recolha de informações antes da atualização

Antes de atualizar, você deve reunir informações para cada um dos nós antigos e, se necessário, ajustar os domínios de broadcast de rede, remover quaisquer VLANs e grupos de interfaces e reunir informações de criptografia.

Sobre esta tarefa

Essa tarefa é executada na configuração MetroCluster FC existente.

Passos

1. Identifique os cabos dos controladores existentes para permitir a identificação fácil dos cabos ao configurar os novos controladores.
2. Reúna as IDs do sistema dos nós na configuração do MetroCluster:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Durante o procedimento de atualização, você substituirá esses IDs de sistema antigos pelos IDs de sistema dos novos módulos de controladora.

   Neste exemplo para uma configuração de FC MetroCluster de quatro nós, as seguintes IDs de sistema antigas são recuperadas:

   - Node_A_1-old: 4068741258
   - Node_A_2-old: 4068741260
   - Node_B_1-old: 4068741254
   - Node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                        node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------ ------------------
-------------                   --------------------
--------------------              ----------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                         4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                         4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                          4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                         4068741260
4068741258
4 entries were displayed.
```

Neste exemplo para uma configuração de FC MetroCluster de dois nós, os seguintes IDs de sistema antigos são recuperados:

- Node_A_1: 4068741258
- Nó_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Reúna informações de porta e LIF para cada nó antigo.

   Você deve reunir a saída dos seguintes comandos para cada nó:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*

- `network port ifgrp show -node node_name -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

4. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves:

   `security key-manager backup show`

6. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações sobre as chaves e senhas.

   Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

   a. Se o Gerenciador de chaves integrado estiver configurado:

      `security key-manager onboard show-backup`

      Você precisará da senha mais tarde no procedimento de atualização.

   b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

      `security key-manager external show -instance`

`security key-manager key query`

Remoção da configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes da transição.

Passos

1. Remova a configuração existente do MetroCluster do software tiebreaker.

"Remoção das configurações do MetroCluster"

2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Enviar uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Para evitar a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a manutenção está em andamento.

   a. Emita o seguinte comando:

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` especifica a duração da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Repita o comando no cluster de parceiros.

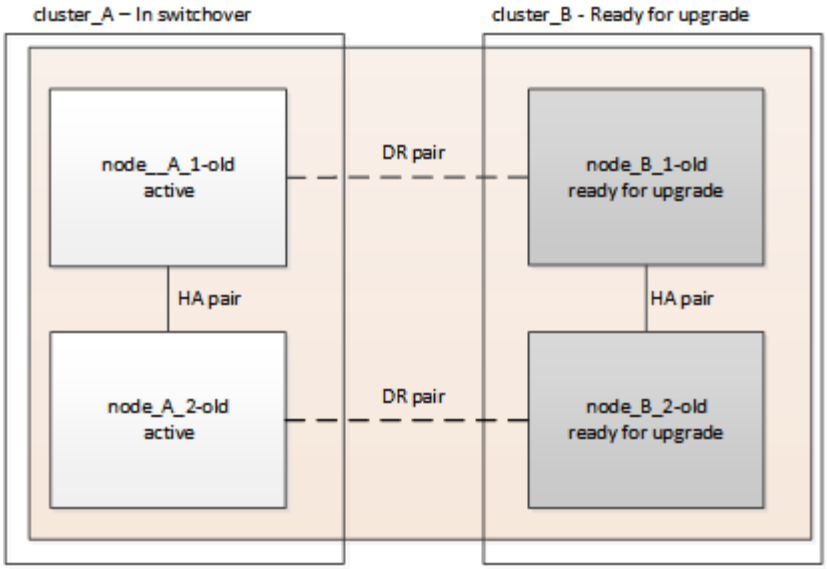
Comutação através da configuração MetroCluster

Você deve alternar a configuração para site_A para que as plataformas no site_B possam ser atualizadas.

Sobre esta tarefa

Esta tarefa tem de ser executada no site_A.

Depois de concluir esta tarefa, o cluster_A está ativo e fornecendo dados para ambos os sites. O cluster_B está inativo e pronto para iniciar o processo de atualização, como mostrado na ilustração a seguir.



Passos

1. Alterne a configuração do MetroCluster para site_A para que os nós do site_B possam ser atualizados:
   a. Selecione a opção que corresponde à sua configuração e emita o comando correto no cluster_A:

      Opção 1: Configuração FC de quatro ou oito nós executando o ONTAP 9.8 ou posterior

      Execute o comando: `metrocluster switchover -controller-replacement true`

      Opção 2: Configuração FC de dois nós executando o ONTAP 9.3 e posterior

      Execute o comando: `metrocluster switchover`

      A operação pode levar vários minutos para ser concluída.

   b. Monitorize a operação de comutação:

      ```
      metrocluster operation show
      ```

   c. Após a conclusão da operação, confirme se os nós estão no estado de comutação:

      ```
      metrocluster show
      ```

   d. Verifique o status dos nós MetroCluster:

      ```
      metrocluster node show
      ```

2. Curar os agregados de dados.
   a. Curar os agregados de dados:

      ```
      metrocluster heal data-aggregates
      ```

   b. Confirme se a operação de cura está concluída executando o `metrocluster operation show` comando no cluster de integridade:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Curar os agregados de raiz.
   a. Curar os agregados de dados:

      `metrocluster heal root-aggregates`

   b. Confirme se a operação de cura está concluída executando o `metrocluster operation show` comando no cluster de integridade:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Preparando a configuração de rede dos controladores antigos

Para garantir que a rede seja retomada de forma limpa nos novos controladores, você deve mover LIFs para uma porta comum e remover a configuração de rede dos controladores antigos.

Sobre esta tarefa

- Esta tarefa deve ser executada em cada um dos nós antigos.
- Você usará as informações coletadas em "Mapeamento de portas dos nós antigos para os novos nós".

Passos

1. Inicialize os nós antigos e faça login nos nós:

   `boot_ontap`

2. Atribua a porta inicial de todas as LIFs de dados no controlador antigo a uma porta comum que seja a mesma nos módulos de controladora antigos e novos.
   a. Apresentar os LIFs:

      `network interface show`

      Todos os LIFS de dados, incluindo SAN e nas, serão administradores acima e operacionalmente inativos, uma vez que eles estão ativos no local de switchover (cluster_A).

   b. Revise a saída para encontrar uma porta de rede física comum que seja a mesma nos controladores

antigos e novos que não seja usada como uma porta de cluster.

Por exemplo, e0d é uma porta física em controladores antigos e também está presente em novos controladores. e0d não é usado como uma porta de cluster ou de outra forma nos novos controladores.

Para obter informações sobre a utilização de portas para modelos de plataforma, consulte a. "NetApp Hardware Universe"

c. Modifique todos os dados LIFS para usar a porta comum como a porta inicial:

`network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

No exemplo a seguir, isso é "e0d".

Por exemplo:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modifique domínios de broadcast para remover vlan e portas físicas que precisam ser excluídas:

`broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

Repita esta etapa para todas as portas VLAN e físicas.

4. Remova quaisquer portas VLAN usando portas de cluster como portas membro e ifgrps usando portas de cluster como portas membro.

a. Eliminar portas VLAN:

`network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

Por exemplo:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remover portas físicas dos grupos de interface:

`network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

Por exemplo:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Remover portas VLAN e grupo de interfaces do domínio de broadcast::

`network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast`

```
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Modifique as portas do grupo de interfaces para usar outras portas físicas como membro, conforme necessário.:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Parar os nós:

```
halt -inhibit-takeover true -node node-name
```

Esta etapa deve ser executada em ambos os nós.

Remover as plataformas antigas

Os controladores antigos devem ser removidos da configuração.

Sobre esta tarefa

Esta tarefa é executada no site_B.

Passos

1. Conete-se ao console serial dos controladores antigos (node_B_1-old e node_B_2-old) no site_B e verifique se ele está exibindo o prompt Loader.
2. Desconete as conexões de storage e rede em node_B_1-old e node_B_2-old e rotule os cabos para que possam ser reconetados aos novos nós.
3. Desconete os cabos de alimentação do node_B_1-old e node_B_2-old.
4. Remova os controladores node_B_1-old e node_B_2-old do rack.

Configurando os novos controladores

Você deve montar e instalar os controladores, executar a configuração necessária no modo de manutenção e, em seguida, inicializar os controladores e verificar a configuração de LIF nos controladores.

Configurando os novos controladores

É necessário colocar em rack e cabo as novas controladoras.

Passos

1. Planeje o posicionamento dos novos módulos de controladora e compartimentos de armazenamento conforme necessário.

   O espaço em rack depende do modelo de plataforma dos módulos de controladora, dos tipos de switch e do número de compartimentos de storage em sua configuração.

2. Aterre-se corretamente.
3. Instale os módulos do controlador no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Se os novos módulos de controladora não tiverem placas FC-VI próprias e se as placas FC-VI de controladoras antigas forem compatíveis com novas controladoras, troque placas FC-VI e instale-as nos

slots corretos.

Consulte "NetApp Hardware Universe"para obter informações sobre o slot para placas FC-VI.

5. Faça o cabeamento das conexões de alimentação, console serial e gerenciamento dos controladores conforme descrito nos guias de instalação e configuração *MetroCluster*.

   Não conete nenhum outro cabo que tenha sido desconetado dos controladores antigos neste momento.

   "Documentação dos sistemas de hardware da ONTAP"

6. Ligue os novos nós e pressione Ctrl-C quando solicitado a exibir o prompt Loader.

Netbooting os novos controladores

Depois de instalar os novos nós, você precisa netboot para garantir que os novos nós estejam executando a mesma versão do ONTAP que os nós originais. O termo netboot significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para netboot, você deve colocar uma cópia da imagem de inicialização do ONTAP 9 em um servidor da Web que o sistema possa acessar.

Esta tarefa é executada em cada um dos novos módulos do controlador.

Passos

1. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.
2. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o ficheiro ONTAP-version_image.tgz num diretório acessível à Web.
3. Vá para o diretório acessível pela Web e verifique se os arquivos que você precisa estão disponíveis.

Se o modelo da plataforma for…	Então…
Sistemas da série FAS/AFF8000	Extraia o conteúdo do arquivo ONTAP-version_image.tgzfile para o diretório de destino: Tar -zxvf ONTAP-version_image.tgz NOTA: Se você estiver extraindo o conteúdo no Windows, use 7-Zip ou WinRAR para extrair a imagem netboot. Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel:netboot/kernel
Todos os outros sistemas	Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel: ONTAP-version_image.tgz você não precisa extrair o arquivo ONTAP-version_image.tgz.

4. No prompt Loader, configure a conexão netboot para um LIF de gerenciamento:
   - Se o endereçamento IP for DHCP, configure a conexão automática:

     ```
     ifconfig e0M -auto
     ```

   - Se o endereçamento IP for estático, configure a conexão manual:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Execute o netboot.

- Se a plataforma for um sistema da série 80xx, use este comando:

  ```
  netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
  ```

- Se a plataforma for qualquer outro sistema, use o seguinte comando:

  ```
  netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
  ```

6. No menu de arranque, selecione a opção **(7) Instalar primeiro o novo software** para transferir e instalar a nova imagem de software no dispositivo de arranque.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se você for solicitado a continuar o procedimento, digite `y` e,
   quando solicitado a fornecer o pacote, digite o URL do arquivo de
   imagem: `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Certifique-se de entrar `n` para ignorar a recuperação de backup quando você vir um prompt semelhante ao seguinte:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Reinicie entrando `y` quando você vir um prompt semelhante ao seguinte:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

Limpando a configuração em um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   ```
   halt
   ```

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

```
set-defaults
```

3. Salvar o ambiente:

```
saveenv
```

4. No prompt DO Loader, inicie o menu de inicialização:

```
boot_ontap menu
```

5. No prompt do menu de inicialização, desmarque a configuração:

```
wipeconfig
```

Responda `yes` ao prompt de confirmação.

O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

Responda `yes` ao prompt de confirmação.

Restaurar a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:

   a. Verifique as definições atuais das portas: `ucadmin show`

   b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
Destino de FC	`fcadmin config -t target` *`adapter-name`*
Iniciador FC	`fcadmin config -t initiator` *`adapter-name`*

2. Sair do modo de manutenção:

```
halt
```

Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

3. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem

em vigor:

```
boot_ontap maint
```

4. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Configuração do estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   ```
   ha-config show
   ```

   O estado de HA para todos os componentes deve ser mcc.

Se a configuração do MetroCluster tiver…	O estado HA deve ser…
Dois nós	mcc-2n
Quatro ou oito nós	mcc

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA para o módulo do controlador e para o chassis:

Se a configuração do MetroCluster tiver…	Emitir estes comandos…
Dois nós	`ha-config modify controller mcc-2n` `ha-config modify chassis mcc-2n`
Quatro ou oito nós	`ha-config modify controller mcc` `ha-config modify chassis mcc`

Reatribuir discos agregados de raiz

Reatribua os discos agregados de raiz ao novo módulo de controladora, usando os sysids reunidos anteriormente

Sobre esta tarefa

Esta tarefa é executada no modo Manutenção.

As IDs de sistema antigas foram identificadas no "Recolha de informações antes da atualização".

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Nó	ID do sistema antigo	Nova ID do sistema
node_B_1	4068741254	1574774970

Passos

1. Cable todas as outras conexões aos novos módulos de controladora (FC-VI, armazenamento, interconexão de cluster, etc.).
2. Interrompa o sistema e inicie para o modo de manutenção a partir do prompt Loader:

   ```
   boot_ontap maint
   ```

3. Exiba os discos de propriedade de node_B_1-old:

   ```
   disk show -a
   ```

   A saída do comando mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (4068741254). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   ...
   ```

4. Reatribua os discos agregados de raiz nas gavetas de unidades à nova controladora:

   `disk reassign -s old-sysid -d new-sysid`

   O exemplo a seguir mostra a reatribuição de unidades:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verifique se todos os discos estão reatribuídos conforme esperado:

   `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Exibir o status agregado:

```
aggr status
```

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Repita as etapas acima no nó do parceiro (node_B_2-novo).

Inicializando os novos controladores

Você deve reiniciar os controladores a partir do menu de inicialização para atualizar a imagem flash do controlador. Etapas adicionais são necessárias se a criptografia estiver configurada.

Sobre esta tarefa

Esta tarefa deve ser executada em todos os novos controladores.

Passos

1. Parar o nó:

```
halt
```

2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

```
setenv bootarg.kmip.init.ipaddr ip-address

setenv bootarg.kmip.init.netmask netmask

setenv bootarg.kmip.init.gateway gateway-address

setenv bootarg.kmip.init.interface interface-id
```

3. Apresentar o menu de arranque:

```
boot_ontap menu
```

4. Se a criptografia raiz for usada, dependendo da versão do ONTAP que você estiver usando, selecione a opção do menu de inicialização ou emita o comando do menu de inicialização para a configuração de gerenciamento de chaves.

ONTAP 9 F.8 e mais tarde

Começando com ONTAP 9.8, selecione a opção do menu de inicialização.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, execute o comando boot menu.

Se você estiver usando…	Emita este comando no prompt do menu de inicialização…
Gerenciamento de chaves integrado	`recover_onboard_keymanager`
Gerenciamento de chaves externas	`recover_external_keymanager`

5. Se o autoboot estiver ativado, interrompa o processo pressionando CTRL-C..

6. No menu de inicialização, execute a opção "'6".

   > A opção "'6" reiniciará o nó duas vezes antes de concluir.

   Responda "y" aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Verifique se o parceiro-sysid está correto:

   ```
   printenv partner-sysid
   ```

   Se o parceiro-sysid não estiver correto, defina-o:

   ```
   setenv partner-sysid partner-sysID
   ```

8. Se a criptografia raiz for usada, dependendo da versão do ONTAP que você estiver usando, selecione a opção do menu de inicialização ou emita o comando do menu de inicialização novamente para a configuração de gerenciamento de chaves.

ONTAP 9 F.8 e mais tarde

Começando com ONTAP 9.8, selecione a opção do menu de inicialização.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

Dependendo da configuração do gerenciador de chaves, execute o procedimento de recuperação selecionando a opção ""10"" ou a opção ""11"", seguida da opção ""6"" no primeiro prompt do menu de inicialização. Para inicializar os nós completamente, você pode precisar repetir o procedimento de recuperação continuado pela opção "'1'" (inicialização normal).

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, execute o comando boot menu.

Se você estiver usando…	Emita este comando no prompt do menu de inicialização…
Gerenciamento de chaves integrado	`recover_onboard_keymanager`
Gerenciamento de chaves externas	`recover_external_keymanager`

Talvez seja necessário emitir o `recover_xxxxxxxx_keymanager` comando no prompt do menu de inicialização várias vezes até que os nós iniciem completamente.

9. Inicialize os nós:

   `boot_ontap`

10. Aguarde que os nós substituídos iniciem.

    Se um dos nós estiver no modo de aquisição, execute um procedimento para giveback:

    `storage failover giveback`

11. Verifique se todas as portas estão em um domínio de broadcast:

    a. Veja os domínios de broadcast:

```
network port broadcast-domain show
```

b. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

"Adicionar ou remover portas de um domínio de broadcast"

c. Adicione a porta física que hospedará as LIFs entre clusters ao domínio Broadcast correspondente.

d. Modifique LIFs entre clusters para usar a nova porta física como porta inicial.

e. Depois que os LIFs entre clusters estiverem ativos, verifique o status de peer do cluster e restabeleça o peering de cluster conforme necessário.

Talvez seja necessário reconfigurar o peering de cluster.

"Criando um relacionamento de cluster peer"

f. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

12. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Verificando a configuração de LIF

Verifique se os LIFs estão hospedados em nós/portas apropriados antes do switchback. As etapas a seguir precisam ser executadas

Sobre esta tarefa

Esta tarefa é executada no site_B, onde os nós foram inicializados com agregados de raiz.

Passos

1. Verifique se os LIFs estão hospedados no nó e nas portas apropriadas antes do switchback.

a. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

b. Substituir a configuração da porta para garantir o posicionamento correto do LIF:

```
vserver config override -command "network interface modify -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node new_node_name"
```

Ao inserir o `network interface modify` comando dentro do `vserver config override` comando, você não pode usar o recurso Tab autocomplete. Você pode criar o `network interface modify` usando autocomplete e, em seguida, incorporá-lo no `vserver config override` comando.

a. Voltar para o nível de privilégio de administrador
`set -privilege admin`

2. Reverter as interfaces para o seu nó inicial:

```
network interface revert * -vserver vserver-name
```

Execute esta etapa em todas as SVMs, conforme necessário.

Instale as novas licenças

Antes da operação de switchback, você deve instalar licenças para os novos controladores.

Passos

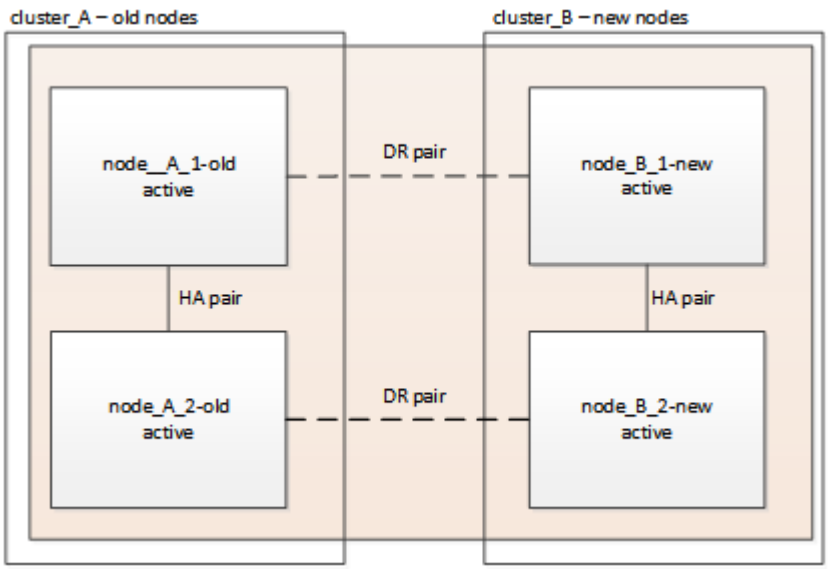
1. "Instalar licenças para o novo módulo de controlador"

Voltando a configurar o MetroCluster

Depois que os novos controladores tiverem sido configurados, a configuração do MetroCluster será reativada para retornar a configuração à operação normal.

Sobre esta tarefa

Nesta tarefa, você executará a operação de switchback, retornando a configuração do MetroCluster à operação normal. Os nós no site_A ainda estão aguardando atualização.



Passos

1. Emita o `metrocluster node show` comando no site_B e verifique a saída.
   a. Verifique se os novos nós estão representados corretamente.
   b. Verifique se os novos nós estão em "aguardando pelo estado de switchback".
2. Comutar o cluster:

   `metrocluster switchback`

3. Verifique o progresso do funcionamento do interrutor de comutação:

   `metrocluster show`

   A operação de switchback ainda está em andamento quando a saída exibe `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   A operação de comutação está concluída quando a saída exibe `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

   Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o `metrocluster config-replication resync-status show` comando. Este comando está no nível de privilégio avançado.

Verificar o estado da configuração do MetroCluster

Depois de atualizar os módulos do controlador, você deve verificar a integridade da configuração do MetroCluster.

Sobre esta tarefa

Esta tarefa pode ser executada em qualquer nó na configuração do MetroCluster.

Passos

1. Verifique o funcionamento da configuração do MetroCluster:

   a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

   b. Execute uma verificação MetroCluster:

      `metrocluster check run`

   c. Apresentar os resultados da verificação MetroCluster:

      `metrocluster check show`

   Depois de executar `metrocluster check run` e `metrocluster check show`, você verá uma mensagem de erro semelhante à seguinte:

   Exemplo

   ```
   Failed to validate the node and cluster components before the switchover
   operation.
                    Cluster_A:: node_A_1 (non-overridable veto): DR
   partner NVLog mirroring is not online. Make sure that the links between
   the two sites are healthy and properly configured.
   ```

   +
   Este comportamento é esperado devido a uma incompatibilidade de controlador durante o processo de atualização e a mensagem de erro pode ser ignorada com segurança.

Atualizando os nós no cluster_A

Você deve repetir as tarefas de atualização no cluster_A.

Passo

1. Repita as etapas para atualizar os nós no cluster_A, começando com "Preparando-se para a atualização".

   À medida que você executa as tarefas, todas as referências de exemplo aos clusters e nós são invertidas. Por exemplo, quando o exemplo é dado para o switchover de cluster_A, você irá mudar de cluster_B.

Enviar uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a atualização, você deve enviar uma mensagem AutoSupport indicando o fim da manutenção, para que a criação automática de casos possa ser retomada.

Passo

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.

a. Emita o seguinte comando:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

b. Repita o comando no cluster de parceiros.

Restaurar a monitorização do desempate

Se a configuração do MetroCluster tiver sido configurada anteriormente para monitoramento pelo software tiebreaker, você poderá restaurar a conexão tiebreaker.

1. Use as etapas em em "Adição de configurações do MetroCluster" *Instalação e Configuração do tiebreaker MetroCluster*.

Atualizar controladores de AFF A700/FAS9000 para AFF A900/FAS9500 em uma configuração MetroCluster FC usando switchover e switchback (ONTAP 9.10,1 ou posterior)

Você pode usar a operação switchover do MetroCluster para fornecer serviços sem interrupções aos clientes enquanto os módulos de controladora no cluster de parceiros são atualizados. Não é possível atualizar outros componentes (como compartimentos de armazenamento ou switches) como parte deste procedimento.

Sobre esta tarefa

- Você pode usar este procedimento apenas para atualização do controlador.

  Não é possível atualizar outros componentes na configuração, como compartimentos de armazenamento ou switches, ao mesmo tempo.

- Pode utilizar este procedimento para atualizar um AFF A700 para o AFF A900 com o ONTAP 9.10,1 e posterior.
- Você pode usar este procedimento para atualizar um FAS9000 para o FAS9500 com o ONTAP 9.10.1P3 e posterior.
  - Configurações de quatro e oito nós são suportadas no ONTAP 9.10,1 e versões posteriores.

    O sistema AFF A900 é suportado apenas no ONTAP 9.10,1 ou posterior.

  "NetApp Hardware Universe"

- Todos os controladores na configuração devem ser atualizados durante o mesmo período de manutenção.

  A tabela a seguir mostra a matriz de modelo suportada para a atualização da controladora.

Modelo de plataforma antigo	Novo modelo de plataforma
• AFF A700	• AFF A900

• FAS9000	• FAS9500

- Durante o procedimento de atualização, você precisa alterar a malha do MetroCluster, incluindo o RCF e alterações físicas do cabeamento. Você pode executar as alterações de RCF e cabeamento antes de executar a atualização da controladora.
- Esse procedimento de atualização não exige que você não altere as conexões de storage, FC e Ethernet entre os nós originais e os novos nós.
- Durante o procedimento de atualização, você não deve adicionar ou remover outras placas do sistema AFF A700 ou FAS9000. Para obter mais informações, consulte a. "NetApp Hardware Universe"

Os nomes de exemplo a seguir são usados em exemplos e gráficos neste procedimento:

- Local_A
  - Antes da atualização:
    - node_A_1-A700
    - node_A_2-A700
  - Após a atualização:
    - node_A_1-A900
    - node_A_2-A900
- Local_B
  - Antes da atualização:
    - node_B_1-A700
    - node_B_2-A700
  - Após a atualização:
    - node_B_1-A900
    - node_B_2-A900

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Prepare-se para a atualização

Antes de fazer alterações na configuração existente do MetroCluster, você deve verificar a integridade da configuração, alterar os arquivos RCF e o cabeamento para corresponder à nova topologia de conectividade de porta necessária para a configuração do AFF A900 ou FAS9000 Fabric MetroCluster e executar outras tarefas diversas.

Limpe a ranhura 7 no controlador AFF A700

A configuração MetroCluster em um AFF A900 ou FAS9500 requer 8 portas FC-VI em placas FC-VI nos slots 5 e 7. Antes de iniciar a atualização, se houver placas no slot 7 no AFF A700 ou no FAS9000, você deve movê-las para outros slots para todos os nós do cluster.

Verifique a integridade da configuração do MetroCluster

Antes de atualizar os arquivos RCF e o cabeamento da configuração AFF A900 ou FAS9500 Fabric MetroCluster, verifique a integridade e a conectividade da configuração.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:

   a. Verifique se os nós são multipathed: Mais
   `node run -node node-name sysconfig -a`

      Você deve emitir este comando para cada nó na configuração do MetroCluster.

   b. Verifique se não há discos quebrados na configuração:

      `storage disk show -broken`

      Você deve emitir este comando em cada nó na configuração do MetroCluster.

   c. Verifique se existem alertas de saúde:

      `system health alert show`

      Você deve emitir este comando em cada cluster.

   d. Verifique as licenças nos clusters:

      `system license show`

      Você deve emitir este comando em cada cluster.

   e. Verifique os dispositivos conetados aos nós:

      `network device-discovery show`

      Você deve emitir este comando em cada cluster.

   f. Verifique se o fuso horário e a hora estão definidos corretamente em ambos os sites:

      `cluster date show`

Você deve emitir este comando em cada cluster. Pode utilizar os `cluster date` comandos para configurar a hora e o fuso horário.

2. Verifique se existem alertas de estado nos interrutores (se presentes):

   `storage switch show`

   Você deve emitir este comando em cada cluster.

3. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

   b. Confirme se todos os nós esperados são mostrados:

      `metrocluster node show`

   c. Emita o seguinte comando:

      `metrocluster check run`

   d. Apresentar os resultados da verificação MetroCluster:

      `metrocluster check show`

4. Verifique o cabeamento do MetroCluster com a ferramenta Config Advisor.
   a. Baixe e execute o Config Advisor.

      "NetApp Downloads: Config Advisor"

   b. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Atualize os arquivos RCF do switch de malha

O AFF A900 ou FAS9500 Fabric MetroCluster requer dois adaptadores FC-VI de quatro portas por nó em comparação com um único adaptador FC-VI de quatro portas exigido por um AFF A700. Antes de iniciar a atualização da controladora para a controladora AFF A900 ou FAS9500, é necessário modificar os arquivos RCF do switch de malha para dar suporte à topologia de conexão AFF A900 ou FAS9500.

1. "Página de download do arquivo MetroCluster RCF"No , faça o download do arquivo RCF correto para um AFF A900 ou FAS9500 Fabric MetroCluster e o modelo de switch que está em uso na configuração AFF A700 ou FAS9000.
2. Atualize o arquivo RCF nos switches Fabric A, switch A1 e switch B1 seguindo as etapas em "Configuração dos switches FC".

   > A atualização do arquivo RCF para dar suporte à configuração AFF A900 ou FAS9500 Fabric MetroCluster não afeta a porta e as conexões usadas para a configuração AFF A700 ou FAS9000 Fabric MetroCluster.

3. Depois de atualizar os arquivos RCF nos switches da malha A, todo o storage e conexões FC-VI devem ficar online. Verifique as conexões FC-VI:

```
metrocluster interconnect mirror show
```

a. Verifique se os discos locais e remotos estão listados na `sysconfig` saída.

4. você deve verificar se o MetroCluster está em um estado saudável após a atualização do arquivo RCF para switches Fabric A.

a. Verifique as conexões do cluster do Metrô:
`metrocluster interconnect mirror show`

b. Execute a verificação MetroCluster:
`metrocluster check run`

c. Veja os resultados da execução do MetroCluster quando a execução for concluída:
`metrocluster check show`

5. Atualize os switches da malha B (switches 2 e 4) repetindo Passo 2 para Passo 5.

Verifique a integridade da configuração do MetroCluster após a atualização do arquivo RCF

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a atualização.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:

a. Verifique se os nós são multipathed: Mais
`node run -node node-name sysconfig -a`

Você deve emitir este comando para cada nó na configuração do MetroCluster.

b. Verifique se não há discos quebrados na configuração:

```
storage disk show -broken
```

Você deve emitir este comando em cada nó na configuração do MetroCluster.

c. Verifique se existem alertas de saúde:

```
system health alert show
```

Você deve emitir este comando em cada cluster.

d. Verifique as licenças nos clusters:

```
system license show
```

Você deve emitir este comando em cada cluster.

e. Verifique os dispositivos conetados aos nós:

```
network device-discovery show
```

Você deve emitir este comando em cada cluster.

f. Verifique se o fuso horário e a hora estão definidos corretamente em ambos os sites:

```
cluster date show
```

Você deve emitir este comando em cada cluster. Pode utilizar os `cluster date` comandos para configurar a hora e o fuso horário.

2. Verifique se existem alertas de estado nos interrutores (se presentes):

```
storage switch show
```

Você deve emitir este comando em cada cluster.

3. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

```
metrocluster show
```

   b. Confirme se todos os nós esperados são mostrados:

```
metrocluster node show
```

   c. Emita o seguinte comando:

```
metrocluster check run
```

   d. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

4. Verifique o cabeamento do MetroCluster com a ferramenta Config Advisor.
   a. Baixe e execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

   b. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Mapeie portas dos nós AFF A700 ou FAS9000 para os nós AFF A900 ou FAS9500

Durante o processo de atualização da controladora, você só deve alterar as conexões mencionadas neste procedimento.

Se os controladores AFF A700 ou FAS9000 tiverem uma placa no slot 7, você deverá movê-la para outro slot antes de iniciar o procedimento de atualização da controladora. Você precisa ter o slot 7 disponível para a adição do segundo adaptador FC-VI necessário para o funcionamento do Fabric MetroCluster nas controladoras AFF A900 ou FAS9500.

Reúna informações antes da atualização

Antes de atualizar, você deve reunir informações para cada um dos nós antigos e, se necessário, ajustar os domínios de broadcast de rede, remover quaisquer VLANs e grupos de interfaces e reunir informações de criptografia.

Sobre esta tarefa

Essa tarefa é executada na configuração MetroCluster FC existente.

Passos

1. Reunir as IDs de sistema do nó de configuração do MetroCluster:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Durante o procedimento de atualização, você substituirá esses IDs de sistema antigos pelos IDs de sistema dos módulos do controlador.

   Neste exemplo para uma configuração de FC MetroCluster de quatro nós, as seguintes IDs de sistema antigas são recuperadas:

   - Node_A_1-A700: 537037649
   - Node_A_2-A700: 537407030
   - Node_B_1-A700: 0537407114
   - Node_B_2-A700: 537035354

```
Cluster_A::*> metrocluster node show -fields node-systemid,ha-partner-
systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id cluster    node           node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ------------------------- ------------- -------------------
------------------- ---------------------
1           Cluster_A  nodeA_1-A700   537407114     537035354
537411005           537410611
1           Cluster_A  nodeA_2-A700   537035354     537407114
537410611           537411005
1           Cluster_B  nodeB_1-A700   537410611     537411005
537035354           537407114
1           Cluster_B  nodeB_2-A700   537411005

4 entries were displayed.
```

2. Reúna informações de porta e LIF para cada nó antigo.

   Você deve reunir a saída dos seguintes comandos para cada nó:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node-name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`

- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

3. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

4. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves:

   `security key-manager backup show`

5. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações sobre as chaves e senhas.

   Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

   a. Se o Gerenciador de chaves integrado estiver configurado:

      `security key-manager onboard show-backup`

      Você precisará da senha mais tarde no procedimento de atualização.

   b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

      `security key-manager external show -instance`

`security key-manager key query`

Remova a configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes da transição.

Passos

1. Remova a configuração existente do MetroCluster do software tiebreaker.

   "Remoção das configurações do MetroCluster"

2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Envie uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Para evitar a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a manutenção está em andamento.

   a. Emita o seguinte comando:

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` especifica a duração da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Repita o comando no cluster de parceiros.

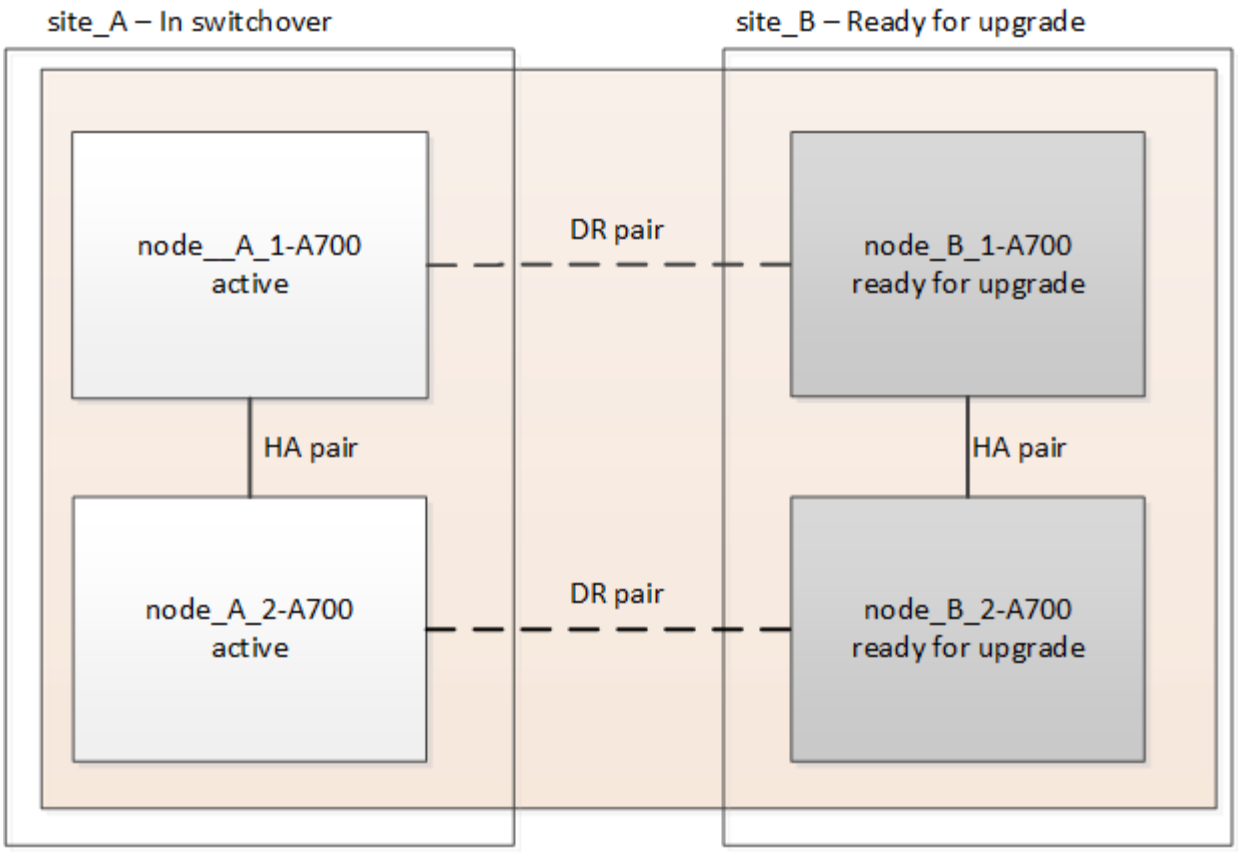
Alterne a configuração do MetroCluster

Você deve alternar a configuração para site_A para que as plataformas no site_B possam ser atualizadas.

Sobre esta tarefa

Esta tarefa tem de ser executada no site_A.

Depois de concluir esta tarefa, site_A está ativo e fornecendo dados para ambos os sites. O Site_B está inativo e pronto para iniciar o processo de atualização, como mostrado na ilustração a seguir. (Esta ilustração também se aplica à atualização de um FAS9000 para um controlador FAS9500.)



Passos

1. Alterne a configuração do MetroCluster para site_A para que os nós do site_B possam ser atualizados:

   a. Execute o seguinte comando no site_A:

   ```
   metrocluster switchover -controller-replacement true
   ```

   A operação pode levar vários minutos para ser concluída.

   a. Monitorize a operação de comutação:

   ```
   metrocluster operation show
   ```

   b. Após a conclusão da operação, confirme se os nós estão no estado de comutação:

   ```
   metrocluster show
   ```

   c. Verifique o status dos nós MetroCluster:

   ```
   metrocluster node show
   ```

2. Curar os agregados de dados.

   a. Curar os agregados de dados:

   ```
   metrocluster heal data-aggregates
   ```

   b. Confirme se a operação de cura está concluída executando o `metrocluster operation show` comando no cluster de integridade:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Curar os agregados de raiz.
   a. Curar os agregados de dados:

      `metrocluster heal root-aggregates`

   b. Confirme se a operação de cura está concluída executando o `metrocluster operation show` comando no cluster de integridade:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Remova o módulo do controlador AFF A700 ou FAS9000 e o NVS no local_B

Você deve remover os controladores antigos da configuração.

Você executa esta tarefa no site_B.

Antes de começar

Se você ainda não está aterrado, aterre-se adequadamente.

Passos

1. Conete-se ao console serial dos controladores antigos (node_B_1-700 e node_B_2-700) no site_B e verifique se ele está exibindo o `LOADER` prompt.
2. Reúna os valores de bootarg de ambos os nós no site_B: `printenv`
3. Desligue o chassis no local_B.

Remova o módulo da controladora e o NVS de ambos os nós no local_B

Retire o módulo do controlador AFF A700 ou FAS9000

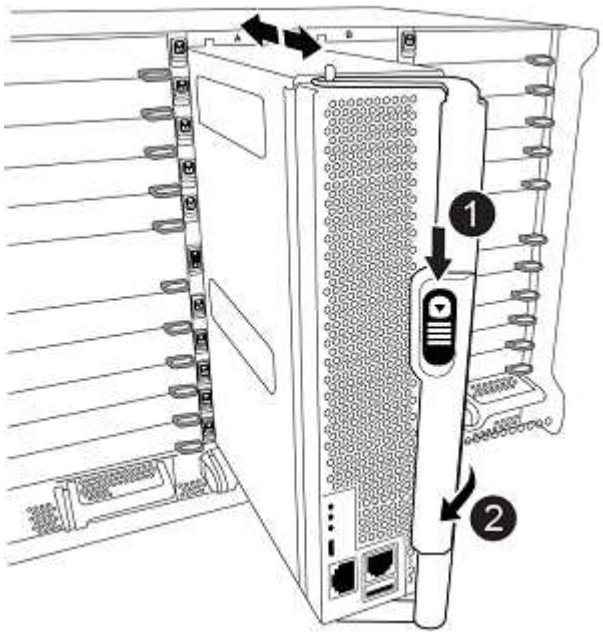
Use o procedimento a seguir para remover o módulo do controlador AFF A700 ou FAS9000.

Passos

1. Retire o cabo da consola, se existir, e o cabo de gestão do módulo do controlador antes de remover o módulo do controlador.

2. Desbloqueie e retire o módulo do controlador do chassis.

   a. Deslize o botão laranja na pega do came para baixo até que este se destranque.



	Botão de libertação do manípulo do excêntrico
	Pega do came

   a. Rode o manípulo do excêntrico de forma a desengatar completamente o módulo do controlador do chassis e, em seguida, deslize o módulo do controlador para fora do chassis. Certifique-se de que suporta a parte inferior do módulo do controlador enquanto o desliza para fora do chassis.

Retire o módulo de ruído, vibração e aspereza (NVS) do AFF A700 ou FAS9000

Use o procedimento a seguir para remover o módulo de ruído, vibração e aspereza (NVS) do AFF A700 ou do FAS9000.

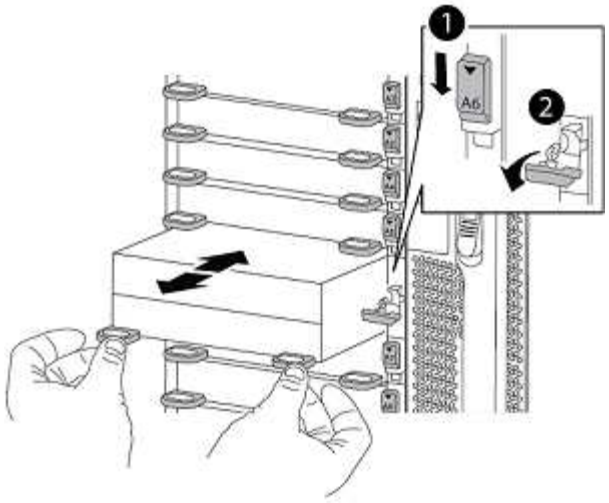
O módulo NVS AFF A700 ou FAS9000 está no slot 6 e é o dobro da altura em comparação com os outros módulos do sistema.

1. Desbloqueie e retire o NVS da ranhura 6.

   a. Prima o botão de came com letras e numerados. O botão do came afasta-se do chassis.

   b. Rode o trinco da árvore de cames para baixo até estar na posição horizontal. O NVS desengata-se do chassis e desloca-se a alguns centímetros.

   c. Retire o NVS do chassis puxando as patilhas de puxar nas laterais da face do módulo.



	Trinco do came de e/S com letras e numerado
	Trinco de e/S completamente desbloqueado

- Não transfira quaisquer módulos adicionais usados como dispositivos de coredump no módulo de armazenamento não volátil AFF A700 no slot 6 para o módulo NVS AFF A900. Não transfira quaisquer peças do controlador AFF A700 e dos módulos NVS para o módulo do controlador AFF A900.
- Para atualizações do FAS9000 para o FAS9500, você deve transferir apenas os módulos do Flash Cache no módulo NVS do FAS9000 para o módulo NVS do FAS9500. Não transfira quaisquer outras peças do controlador FAS9000 e dos módulos NVS para o módulo do controlador FAS9500.

Instale o AFF A900 ou o módulo do controlador NVS e o NVS do FAS9500

Você deve instalar o AFF A900 ou o FAS9500 NVS e o módulo da controladora a partir do kit de atualização em ambos os nós no local_B. Não mova o dispositivo de coredump do módulo NVS AFF A700 ou FAS9000 para o módulo NVS AFF A900 ou FAS9500.

Antes de começar

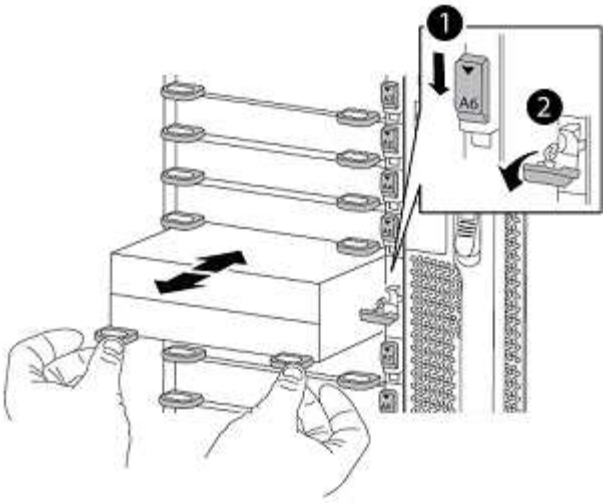
Se você ainda não está aterrado, aterre-se adequadamente.

Instale o AFF A900 ou o FAS9500 NVS

Use o procedimento a seguir para instalar o AFF A900 ou o FAS9500 NVS no slot 6 de ambos os nós no local_B

Passos

1. Alinhe o NVS com as bordas da abertura do chassi no slot 6.
2. Deslize suavemente o NVS para dentro da ranhura até que o trinco do came de e/S com letras e numerado comece a engatar com o pino do came de e/S e, em seguida, empurre o trinco do came de e/S totalmente para cima para bloquear o NVS no devido lugar.



	Trinco do came de e/S com letras e numerado
	Trinco de e/S completamente desbloqueado

Instale o módulo do controlador AFF A900 ou FAS9500

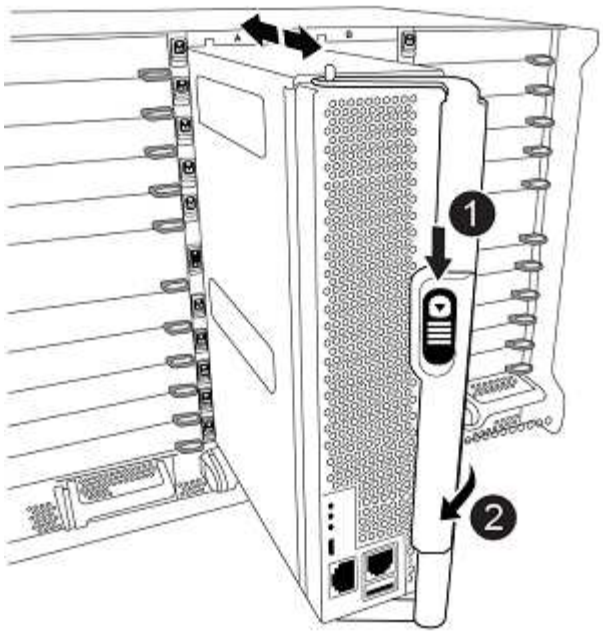
Use o procedimento a seguir para instalar o módulo do controlador AFF A900 ou FAS9500.

Passos

1. Alinhe a extremidade do módulo do controlador com a abertura no chassis e, em seguida, empurre cuidadosamente o módulo do controlador até meio do sistema.
2. Empurre firmemente o módulo do controlador para dentro do chassi até que ele atenda ao plano médio e esteja totalmente assentado. O trinco de bloqueio sobe quando o módulo do controlador está totalmente assente.

   Não utilize força excessiva ao deslizar o módulo do controlador para dentro do chassis para evitar danificar os conetores.

3. Cable as portas de gerenciamento e console ao módulo do controlador.



	Botão de libertação do manípulo do excêntrico
	Pega do came

4. Instale a segunda placa X91129A no slot 7 de cada nó.
   a. Conete as portas FC-VI do slot 7 aos switches. Consulte "Instalação e configuração conectadas à malha" a documentação e acesse os requisitos de conexão AFF A900 ou FAS9500 Fabric MetroCluster para saber o tipo de switch no seu ambiente.
5. LIGUE o chassi e conete ao console serial.
6. Após a inicialização do BIOS, se o nó começar a funcionar em autoboot, interrompa o AUTOBOOT pressionando Control-C.
7. Depois de interromper o autoboot, os nós param no prompt DO Loader. Se você não interromper o serviço em tempo hábil e o node1 começar a inicializar, aguarde que o prompt pressione Control-C para entrar no menu de inicialização. Depois que o nó parar no menu de inicialização, use a opção 8 para reinicializar o nó e interromper o autoboot durante a reinicialização.
8. `LOADER`No prompt, defina as variáveis de ambiente padrão: `set-defaults`
9. Salve as configurações de variáveis de ambiente padrão: `saveenv`

Netboot os nós no site_B

Depois de trocar o módulo de controladora AFF A900 ou FAS9500 e o NVS, você precisa netboot dos nós AFF A900 ou FAS9500 e instalar a mesma versão do ONTAP e o nível de patch que está sendo executado no cluster. O termo `netboot` significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para `netboot`, você deve adicionar uma cópia da imagem de inicialização do ONTAP 9 a um servidor da Web que o sistema possa acessar.

Não é possível verificar a versão do ONTAP instalada no suporte de arranque de um módulo controlador AFF A900 ou FAS9500, a menos que esteja instalado num chassis e ligado. A versão do ONTAP na Mídia de inicialização do AFF A900 ou do FAS9500 deve ser igual à versão do ONTAP executada no sistema AFF

A700 ou FAS9000 que está sendo atualizada e as imagens de inicialização principal e de backup devem corresponder. Pode configurar as imagens executando um `netboot` comando seguido do `wipeconfig` menu de arranque. Se o módulo do controlador foi usado anteriormente em outro cluster, o `wipeconfig` comando limpa qualquer configuração residual na Mídia de inicialização.

Antes de começar

- Verifique se você pode acessar um servidor HTTP com o sistema.
- Você precisa baixar os arquivos de sistema necessários para o seu sistema e a versão correta do ONTAP a partir "Suporte à NetApp"do site. Sobre esta tarefa, você deve `netboot` os novos controladores se a versão do ONTAP instalada não for a mesma que a versão instalada nos controladores originais. Depois de instalar cada novo controlador, inicialize o sistema a partir da imagem ONTAP 9 armazenada no servidor Web. Em seguida, pode transferir os ficheiros corretos para o dispositivo multimédia de arranque para as subsequentes inicializações do sistema.

Passos

1. Acesso "Suporte à NetApp" para baixar os arquivos necessários para executar um netboot do sistema usado para executar o netboot do sistema.
2. Baixe o software ONTAP apropriado na seção de download de software do site de suporte da NetApp e armazene o `<ontap_version>_image.tgz` arquivo em um diretório acessível pela Web.
3. Mude para o diretório acessível pela Web e verifique se os arquivos necessários estão disponíveis. Sua lista de diretórios deve conter `<ontap_version>_image.tgz`.
4. Configure `netboot` a conexão escolhendo uma das seguintes ações. Observação: Você deve usar a porta de gerenciamento e o IP como `netboot` conexão. Não use um IP de LIF de dados ou uma interrupção de dados pode ocorrer enquanto a atualização está sendo realizada.

Se o DHCP (Dynamic Host Configuration Protocol) for…	Então…
Em execução	Configure a conexão automaticamente usando o seguinte comando no prompt do ambiente de inicialização: `ifconfig e0M -auto`
Não está a funcionar	Configure manualmente a conexão usando o seguinte comando no prompt do ambiente de inicialização: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> -dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` É o endereço IP do sistema de armazenamento. `<netmask>` é a máscara de rede do sistema de armazenamento. `<gateway>` é o gateway para o sistema de armazenamento. `<dns_addr>` É o endereço IP de um servidor de nomes na rede. Este parâmetro é opcional. `<dns_domain>` É o nome de domínio do serviço de nomes de domínio (DNS). Este parâmetro é opcional. NOTA: Outros parâmetros podem ser necessários para a sua interface. Digite help ifconfig no prompt do firmware para obter detalhes.

5. Executar `netboot` no nó 1:
`netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`
O `<path_to_the_web-accessible_directory>` deve levar ao local onde você baixou o `<ontap_version>_image.tgz` em Passo 2.

   Não interrompa a inicialização.

6. Aguarde que o nó 1 que está sendo executado no módulo controlador AFF A900 ou FAS9500 inicialize e exiba as opções do menu de inicialização, conforme mostrado abaixo:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

7. No menu de inicialização, selecione a opção `(7) Install new software first`. Esta opção de menu transfere e instala a nova imagem ONTAP no dispositivo de arranque.

   Ignore a seguinte mensagem: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`. Esta observação se aplica a atualizações de software ONTAP sem interrupções e não atualizações de controladora. Sempre use netboot para atualizar o novo nó para a imagem desejada. Se você usar outro método para instalar a imagem no novo controlador, a imagem incorreta pode ser instalada. Este problema aplica-se a todas as versões do ONTAP.

8. Se você for solicitado a continuar o procedimento, digite `y` e, quando solicitado, digite o URL:

   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

9. Conclua as seguintes subetapas para reinicializar o módulo do controlador:

   a. Introduza `n` para ignorar a recuperação da cópia de segurança quando vir o seguinte aviso:
   `Do you want to restore the backup configuration now? {y|n}`

   b. Digite `y` para reiniciar quando você vir o seguinte prompt:
   `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`

O módulo do controlador reinicializa, mas pára no menu de inicialização porque o dispositivo de inicialização foi reformatado e os dados de configuração precisam ser restaurados.

10. No prompt, execute o `wipeconfig` comando para limpar qualquer configuração anterior na Mídia de inicialização:
    a. Quando vir a mensagem abaixo, responda `yes`:
    `This will delete critical system configuration, including cluster membership.`
    `Warning: do not run this option on a HA node that has been taken over.`
    `Are you sure you want to continue?:`
    b. O nó reinicializa para terminar o `wipeconfig` e, em seguida, pára no menu de inicialização.
11. Selecione a opção `5` para ir para o modo de manutenção a partir do menu de arranque. Responda `yes` aos prompts até que o nó pare no modo de manutenção e no prompt de comando `*>` .

Restaure a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:
    a. Verifique as definições atuais das portas: `ucadmin show`
    b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
Destino de FC	`fcadmin config -t target` *`adapter-name`*
Iniciador FC	`fcadmin config -t initiator` *`adapter-name`*

Defina o estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

    `ha-config show`

    O estado de HA para todos os componentes deve ser mcc.

2. Se o estado do sistema apresentado do controlador ou do chassis não estiver correto, defina o estado HA:

   `ha-config modify controller mcc`

   `ha-config modify chassis mcc`

3. Parar o nó: `halt` O nó deve parar no `LOADER>` prompt.
4. Em cada nó, verifique a data, a hora e o fuso horário do sistema: `Show date`
5. Se necessário, defina a data em UTC ou Greenwich Mean Time (GMT): `set date <mm/dd/yyyy>`
6. Verifique a hora usando o seguinte comando no prompt do ambiente de inicialização: `show time`
7. Se necessário, defina a hora em UTC ou GMT: `set time <hh:mm:ss>`
8. Guarde as definições: `saveenv`
9. Reunir variáveis de ambiente: `printenv`
10. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:
    `boot_ontap maint`
11. Verifique se as alterações feitas estão efetivas e o ucadmin mostra as portas do iniciador de FC on-line.

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

12. Verifique o modo ha-config: `ha-config show`
    a. Verifique se você tem a seguinte saída:

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Defina o estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado de HA para todos os componentes deve ser mcc.

Se a configuração do MetroCluster tiver…	O estado HA deve ser…

Dois nós	mcc-2n
Quatro ou oito nós	mcc

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA para o módulo do controlador e para o chassis:

Se a configuração do MetroCluster tiver…	Emitir estes comandos…
Dois nós	`ha-config modify controller mcc-2n` `ha-config modify chassis mcc-2n`
Quatro ou oito nós	`ha-config modify controller mcc` `ha-config modify chassis mcc`

Reatribuir discos agregados de raiz

Reatribua os discos agregados de raiz ao novo módulo de controladora, usando os sysids reunidos anteriormente

Sobre esta tarefa

Esta tarefa é executada no modo Manutenção.

As IDs de sistema antigas foram identificadas no "Recolha de informações antes da atualização".

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Nó	ID do sistema antigo	Nova ID do sistema
node_B_1	4068741254	1574774970

Passos

1. Cable todas as outras conexões aos novos módulos de controladora (FC-VI, armazenamento, interconexão de cluster, etc.).
2. Interrompa o sistema e inicie para o modo de manutenção a partir do `LOADER` prompt:

   ```
   boot_ontap maint
   ```

3. Exiba os discos de propriedade do node_B_1-A700:

   ```
   disk show -a
   ```

   A saída de exemplo mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (4068741254). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
...
```

4. Reatribua os discos agregados de raiz nas gavetas de unidades à nova controladora:

   `disk reassign -s old-sysid -d new-sysid`

   O exemplo a seguir mostra a reatribuição de unidades:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verifique se todos os discos estão reatribuídos conforme esperado: `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. Exibir o status agregado: `aggr status`

```
*> aggr status
           Aggr             State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Repita as etapas acima no nó do parceiro (node_B_2-A900).

Inicialize os novos controladores

Você deve reiniciar os controladores a partir do menu de inicialização para atualizar a imagem flash do controlador. Etapas adicionais são necessárias se a criptografia estiver configurada.

Sobre esta tarefa

Esta tarefa deve ser executada em todos os novos controladores.

Passos

1. Parar o nó: `halt`
2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Apresentar o menu de arranque: `boot_ontap menu`
4. Se a criptografia raiz for usada, emita o comando boot menu para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção 10 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves
Gerenciamento de chaves externas	Opção 11 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves

5. Se a função autoboot estiver ativada, interrompa a operação pressionando Control-C..
6. No menu de arranque, execute a opção (6).

A opção 6 reiniciará o nó duas vezes antes de concluir.

Responda `y` aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Verifique se o parceiro-sysid está correto: `printenv partner-sysid`

   Se o parceiro-sysid não estiver correto, defina-o: `setenv partner-sysid` *`partner-sysID`*

8. Se a criptografia raiz for usada, emita o comando boot menu novamente para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção 10 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves
Gerenciamento de chaves externas	Opção 11 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves

   Talvez seja necessário emitir o `recover_xxxxxxxx_keymanager` comando no prompt do menu de inicialização várias vezes até que os nós iniciem completamente.

9. Inicialize os nós: `boot_ontap`
10. Aguarde que os nós substituídos iniciem.

    Se um dos nós estiver no modo de aquisição, execute um giveback usando o `storage failover giveback` comando.

11. Verifique se todas as portas estão em um domínio de broadcast:

    a. Veja os domínios de broadcast:

       `network port broadcast-domain show`

    b. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

       "Adicionar ou remover portas de um domínio de broadcast"

    c. Adicione a porta física que hospedará as LIFs entre clusters ao domínio Broadcast correspondente.

    d. Modifique LIFs entre clusters para usar a nova porta física como porta inicial.

    e. Depois que os LIFs entre clusters estiverem ativos, verifique o status de peer do cluster e restabeleça o peering de cluster conforme necessário.

Talvez seja necessário reconfigurar o peering de cluster.

"Criando um relacionamento de cluster peer"

f. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

12. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Verifique a configuração do LIF

Verifique se os LIFs estão hospedados em nós/portas apropriados antes do switchback. As etapas a seguir precisam ser executadas

Sobre esta tarefa

Esta tarefa é executada no site_B, onde os nós foram inicializados com agregados de raiz.

Passos

1. Verifique se os LIFs estão hospedados no nó e nas portas apropriadas antes do switchback.

a. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

b. Substituir a configuração da porta para garantir o posicionamento correto do LIF:

```
vserver config override -command "network interface modify" -vserver
vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
new_node_name"
```

Ao inserir o `network interface modify` comando dentro do `vserver config override` comando, você não pode usar o recurso Tab autocomplete. Você pode criar o `network interface modify` usando autocomplete e, em seguida, incorporá-lo no `vserver config override` comando.

a. Voltar para o nível de privilégio de administrador

```
set -privilege admin
```

2. Reverter as interfaces para o seu nó inicial:

```
network interface revert * -vserver vserver-name
```

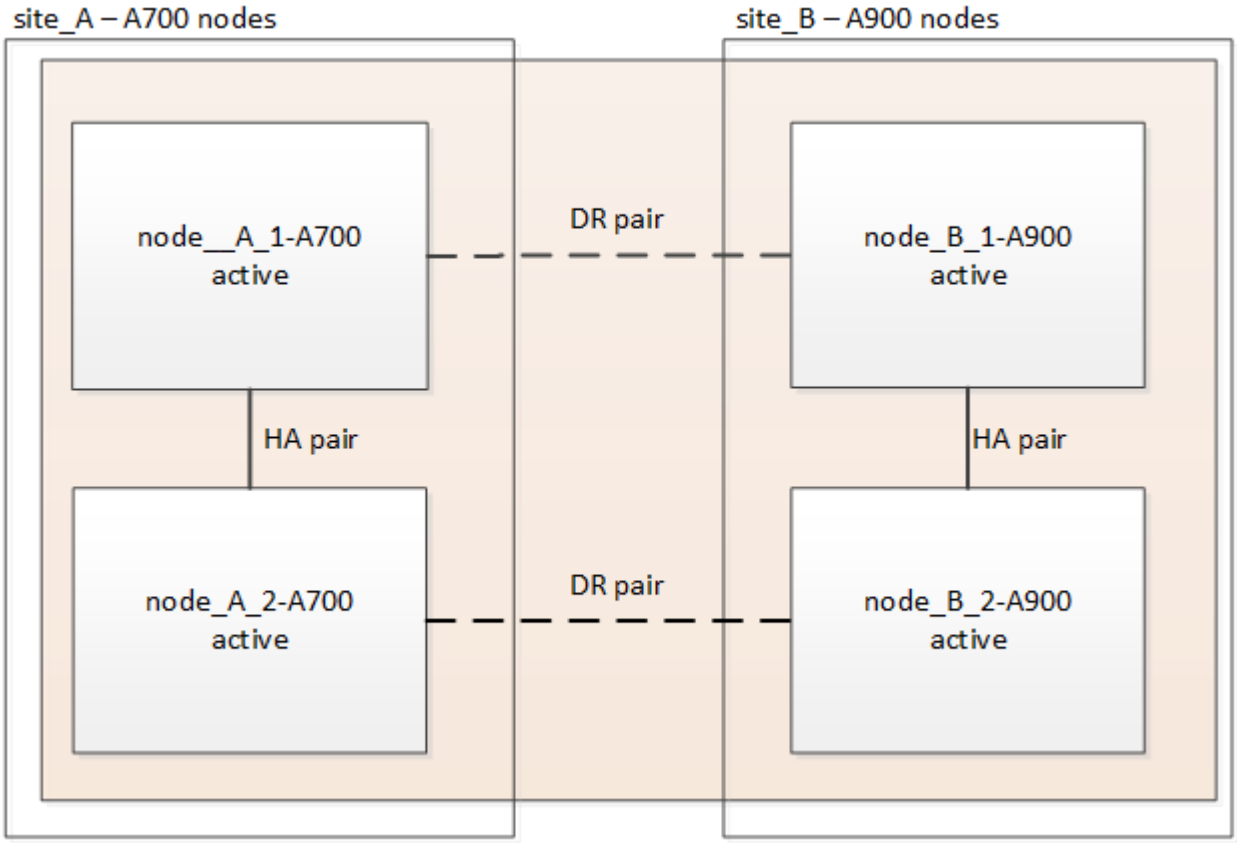
Execute esta etapa em todas as SVMs, conforme necessário.

Volte a ativar a configuração do MetroCluster

Depois que os novos controladores tiverem sido configurados, a configuração do MetroCluster será reativada para retornar a configuração à operação normal.

Sobre esta tarefa

Nesta tarefa, você executará a operação de switchback, retornando a configuração do MetroCluster à operação normal. Os nós no site_A ainda estão aguardando atualização, como mostrado na ilustração a seguir. (Esta ilustração também se aplica à atualização de um FAS9000 para um controlador FAS9500).



Passos

1. Emita o `metrocluster node show` comando no site_B e verifique a saída.
   a. Verifique se os novos nós estão representados corretamente.
   b. Verifique se os novos nós estão em "aguardando pelo estado de switchback".
2. Comutar o cluster:

```
metrocluster switchback
```

3. Verifique o progresso do funcionamento do interrutor de comutação:

   `metrocluster show`

   A operação de switchback ainda está em andamento quando a saída exibe `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   A operação de comutação está concluída quando a saída exibe `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

   Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o `metrocluster config-replication resync-status show` comando. Este comando está no nível de privilégio avançado.

Verifique a integridade da configuração do MetroCluster

Depois de atualizar os módulos do controlador, você deve verificar a integridade da configuração do MetroCluster.

Sobre esta tarefa

Esta tarefa pode ser executada em qualquer nó na configuração do MetroCluster.

Passos

1. Verifique o funcionamento da configuração do MetroCluster:

   a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      `metrocluster show`

b. Execute uma verificação MetroCluster:

```
metrocluster check run
```

c. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

Depois de executar os `metrocluster check run` comandos e `metrocluster check show`, poderá ver um erro semelhante ao seguinte exemplo:

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+
Este erro ocorre devido a uma incompatibilidade de controlador durante o processo de atualização. Você pode ignorar com segurança o erro e continuar a atualizar os nós no site_A.

Atualize os nós no site_A

Você deve repetir as tarefas de atualização no site_A.

Passo

1. Repita as etapas para atualizar os nós no site_A, começando com "Prepare-se para a atualização".

   À medida que você executa as tarefas, todas as referências de exemplo aos sites e nós são invertidas. Por exemplo, quando o exemplo é dado para o switchover de site_A, você irá mudar de Site_B.

Envie uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a atualização, você deve enviar uma mensagem AutoSupport indicando o fim da manutenção, para que a criação automática de casos possa ser retomada.

Passo

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.
   a. Emita o seguinte comando:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   b. Repita o comando no cluster de parceiros.

Restaure o monitoramento do tiebreaker

Se a configuração do MetroCluster tiver sido configurada anteriormente para monitoramento pelo software tiebreaker, você poderá restaurar a conexão tiebreaker.

1. Siga as etapas em: "Adição de configurações do MetroCluster" Na seção *MetroCluster Tiebreaker Installation and Configuration*.

Atualização de controladores em uma configuração MetroCluster FC de quatro nós usando switchover e switchback com os comandos "System controller replace" (ONTAP 9.10,1 e posterior)

Você pode usar essa operação de switchover automatizado guiado por MetroCluster para executar uma atualização sem interrupções do controlador em uma configuração de FC MetroCluster de quatro nós. Outros componentes (como prateleiras de armazenamento ou switches) não podem ser atualizados como parte deste procedimento.

Combinações de plataformas suportadas

- Para obter informações sobre quais combinações de atualização de plataforma são suportadas, consulte a tabela de atualização do MetroCluster FC no "Escolha um procedimento de atualização da controladora".

"Escolher um método de atualização ou atualização"Consulte para obter mais procedimentos.

Sobre esta tarefa

- Você pode usar este procedimento apenas para atualização do controlador.

  Outros componentes na configuração, como compartimentos de armazenamento ou switches, não podem ser atualizados ao mesmo tempo.

- Este procedimento se aplica a módulos do controlador em uma configuração MetroCluster FC de quatro nós.
- As plataformas devem estar executando o ONTAP 9.10,1 ou posterior.

  "NetApp Hardware Universe"

- Você pode usar este procedimento para atualizar controladores em uma configuração MetroCluster FC de quatro nós usando o switchover automatizado baseado em NSO e o switchback. Se você quiser realizar uma atualização de controladora usando ARL (Aggregate Relocation), "Use os comandos "System controller replace" para atualizar o hardware da controladora executando o ONTAP 9.8 ou posterior"consulte . Recomenda-se a utilização do procedimento automatizado baseado em NSO.
- Se os seus sites da MetroCluster estiverem fisicamente em dois locais diferentes, você deve usar o procedimento de atualização automática do controlador NSO para atualizar os controladores em ambos os locais em sequência.
- Esse procedimento automatizado de atualização de controladora baseada em NSO oferece a capacidade de iniciar a substituição da controladora para um local de recuperação de desastres (DR) da MetroCluster. Você só pode iniciar uma substituição de controlador em um local de cada vez.
- Para iniciar uma substituição de controladora no local A, você precisa executar o comando de inicialização de substituição de controladora a partir do local B. a operação orienta você a substituir os controladores de ambos os nós apenas no local A. Para substituir os controladores no local B, é necessário executar o comando de inicialização de substituição do controlador do local A. Uma mensagem é exibida identificando o local no qual os controladores estão sendo substituídos.

Os seguintes nomes de exemplo são usados neste procedimento:

- Local_A
  - Antes da atualização:
    - Node_A_1-old
    - Node_A_2-old
  - Após a atualização:
    - Node_A_1-novo
    - Node_A_2-novo
- Local_B
  - Antes da atualização:
    - Node_B_1-old
    - Node_B_2-old
  - Após a atualização:
    - Node_B_1-novo
    - Node_B_2-novo

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Preparando-se para a atualização

Para se preparar para a atualização da controladora, é necessário realizar pré-verificações do sistema e coletar as informações de configuração.

Em qualquer estágio durante a atualização, você pode executar o `system controller replace show` comando ou `system controller replace show-details` do site A para verificar o status. Se os comandos devolverem uma saída em branco, aguarde alguns minutos e execute novamente o comando.

Passos

1. Inicie o procedimento de substituição automática do controlador A partir do local A para substituir os controladores no local B:

   ```
   system controller replace start
   ```

   A operação automatizada executa as pré-verificações. Se não forem encontrados problemas, a operação

será interrompida para que você possa coletar manualmente as informações relacionadas à configuração.

> O sistema de origem atual e todos os sistemas de destino compatíveis são apresentados. Se você substituiu o controlador de origem por um controlador que tenha uma versão diferente do ONTAP ou uma plataforma não compatível, a operação de automação pára e relata um erro após os novos nós serem inicializados. Para voltar a colocar o cluster num estado saudável, tem de seguir o procedimento de recuperação manual.

O `system controller replace start` comando pode relatar o seguinte erro de pré-verificação:

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- -------------- -------------------------------------
Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

Verifique se esse erro ocorreu porque você tem agregados sem espelhamento ou devido a outro problema agregado. Verifique se todos os agregados espelhados estão saudáveis e não degradados ou degradados por espelho. Se esse erro for devido apenas a agregados sem espelhamento, você pode substituir esse erro selecionando a `-skip-metrocluster-check true` opção no `system controller replace start` comando. Se o storage remoto estiver acessível, os agregados sem espelhamento estarão online após o switchover. Se o link de storage remoto falhar, os agregados sem espelhamento não estarão online.

2. Colete manualmente as informações de configuração fazendo login no local B e seguindo os comandos listados na mensagem do console sob o `system controller replace show` comando ou `system controller replace show-details`.

Recolha de informações antes da atualização

Antes de atualizar, se o volume raiz estiver criptografado, você deverá reunir a chave de backup e outras informações para inicializar os novos controladores com os antigos volumes de raiz criptografados.

Sobre esta tarefa

Essa tarefa é executada na configuração MetroCluster FC existente.

Passos

1. Identifique os cabos dos controladores existentes para que possa identificar facilmente os cabos ao configurar os novos controladores.
2. Exiba os comandos para capturar a chave de backup e outras informações:

   `system controller replace show`

   Execute os comandos listados sob o `show` comando do cluster de parceiros.

3. Reúna as IDs do sistema dos nós na configuração do MetroCluster:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Durante o procedimento de atualização, você substituirá esses IDs de sistema antigos pelos IDs de

sistema dos novos módulos de controladora.

Neste exemplo para uma configuração de FC MetroCluster de quatro nós, as seguintes IDs de sistema antigas são recuperadas:

- Node_A_1-old: 4068741258
- Node_A_2-old: 4068741260
- Node_B_1-old: 4068741254
- Node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

Neste exemplo para uma configuração de FC MetroCluster de dois nós, os seguintes IDs de sistema antigos são recuperados:

- Node_A_1: 4068741258
- Nó_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Reúna informações de porta e LIF para cada nó antigo.

   Você deve reunir a saída dos seguintes comandos para cada nó:

   - `network interface show -role cluster,node-mgmt`

- `network port show -node node-name -type physical`
- `network port vlan show -node node-name`
- `network port ifgrp show -node node_name -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

5. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves:

   `security key-manager backup show`

7. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações sobre as chaves e senhas.

   Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

   a. Se o Gerenciador de chaves integrado estiver configurado:

      `security key-manager onboard show-backup`

      Você precisará da senha mais tarde no procedimento de atualização.

   b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

      `security key-manager external show -instance`

   `security key-manager key query`

8. Depois de concluir a recolha das informações de configuração, retome a operação:

   `system controller replace resume`

Remoção da configuração existente do tiebreaker ou de outro software de monitoramento

Se a configuração existente for monitorada com a configuração tiebreaker do MetroCluster ou outros aplicativos de terceiros (por exemplo, o ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do tiebreaker ou de outro software antes de substituir a controladora antiga.

Passos

1. "Remova a configuração existente do MetroCluster" Do software tiebreaker.
2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Substituindo os controladores antigos e inicializando os novos controladores

Depois de reunir informações e retomar a operação, a automação prossegue com a operação de comutação.

Sobre esta tarefa

A operação de automação inicia as operações de comutação, `heal-aggregates`, e `heal root-aggregates` . Depois que essas operações forem concluídas, a operação será interrompida em **pausado para intervenção do usuário** para que você possa montar e instalar os controladores, inicializar os controladores do parceiro e reatribuir os discos agregados raiz ao novo módulo do controlador a partir do backup flash usando o `sysids` coletado anteriormente.

Antes de começar

Antes de iniciar o switchover, a operação de automação é interrompida para que você possa verificar manualmente se todos os LIFs estão "up" no local B. se necessário, traga quaisquer LIFs que são "próprios" para "'up" e retome a operação de automação usando o `system controller replace resume` comando.

Preparando a configuração de rede dos controladores antigos

Para garantir que a rede seja retomada de forma limpa nos novos controladores, você deve mover LIFs para uma porta comum e remover a configuração de rede dos controladores antigos.

Sobre esta tarefa

- Esta tarefa deve ser executada em cada um dos nós antigos.
- Você usará as informações coletadas em Preparando-se para a atualização.

Passos

1. Inicialize os nós antigos e faça login nos nós:

   ```
   boot_ontap
   ```

2. Atribua a porta inicial de todas as LIFs de dados no controlador antigo a uma porta comum que seja a mesma nos módulos de controladora antigos e novos.

   a. Apresentar os LIFs:

      ```
      network interface show
      ```

      Todos os dados LIFS, incluindo SAN e nas, serão administradores e operacionais "próprios", uma vez que eles estão ativos no local de comutação (cluster_A).

b. Revise a saída para encontrar uma porta de rede física comum que seja a mesma nos controladores antigos e novos que não seja usada como uma porta de cluster.

   Por exemplo, "'e0d'" é uma porta física em controladores antigos e também está presente em novos controladores. "e0d" não é usado como uma porta de cluster ou de outra forma nos novos controladores.

   Para obter informações sobre a utilização de portas para modelos de plataforma, consulte a. "NetApp Hardware Universe"

c. Modifique todos os dados LIFS para usar a porta comum como a porta inicial:

   `network interface modify -vserver svm-name -lif data-lif -home-port port-id`

   No exemplo a seguir, isso é ""e0d"".

   Por exemplo:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modifique domínios de broadcast para remover VLAN e portas físicas que precisam ser excluídas:

   `broadcast-domain remove-ports -broadcast-domain broadcast-domain-name -ports node-name:port-id`

   Repita esta etapa para todas as portas VLAN e físicas.

4. Remova quaisquer portas VLAN usando portas de cluster como portas membros e grupos de interfaces usando portas de cluster como portas membros.

   a. Eliminar portas VLAN:

      `network port vlan delete -node node-name -vlan-name portid-vlandid`

      Por exemplo:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

   b. Remover portas físicas dos grupos de interface:

      `network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

      Por exemplo:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

   a. Remova as portas VLAN e grupo de interfaces do domínio de broadcast:

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Modifique as portas do grupo de interfaces para usar outras portas físicas como membro, conforme necessário.:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Parar os nós:

```
halt -inhibit-takeover true -node node-name
```

Esta etapa deve ser executada em ambos os nós.

Configurando os novos controladores

É necessário colocar em rack e cabo as novas controladoras.

Passos

1. Planeje o posicionamento dos novos módulos de controladora e compartimentos de armazenamento conforme necessário.

   O espaço em rack depende do modelo de plataforma dos módulos de controladora, dos tipos de switch e do número de compartimentos de storage em sua configuração.

2. Aterre-se corretamente.
3. Instale os módulos do controlador no rack ou gabinete.

   "Documentação dos sistemas de hardware da ONTAP"

4. Se os novos módulos de controladora não tiverem placas FC-VI próprias e se as placas FC-VI de controladoras antigas forem compatíveis com novas controladoras, troque placas FC-VI e instale-as nos slots corretos.

   Consulte "NetApp Hardware Universe"para obter informações sobre o slot para placas FC-VI.

5. Faça o cabeamento das conexões de alimentação, console serial e gerenciamento dos controladores conforme descrito nos guias de instalação e configuração *MetroCluster*.

   Não conete nenhum outro cabo que tenha sido desconetado dos controladores antigos neste momento.

   "Documentação dos sistemas de hardware da ONTAP"

6. Ligue os novos nós e pressione Ctrl-C quando solicitado a exibir o prompt Loader.

Netbooting os novos controladores

Depois de instalar os novos nós, você precisa netboot para garantir que os novos nós estejam executando a mesma versão do ONTAP que os nós originais. O termo netboot significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para netboot, você deve colocar uma cópia da imagem de inicialização do ONTAP 9 em um servidor da Web que o sistema possa acessar.

Esta tarefa é executada em cada um dos novos módulos do controlador.

Passos

1. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.
2. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o ficheiro ONTAP-version_image.tgz num diretório acessível à Web.
3. Vá para o diretório acessível pela Web e verifique se os arquivos que você precisa estão disponíveis.

Se o modelo da plataforma for…	Então…
Sistemas da série FAS/AFF8000	Extraia o conteúdo do arquivo ONTAP-version_image.tgzfile para o diretório de destino: Tar -zxvf ONTAP-version_image.tgz NOTA: Se você estiver extraindo o conteúdo no Windows, use 7-Zip ou WinRAR para extrair a imagem netboot. Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel:netboot/kernel
Todos os outros sistemas	Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel: ONTAP-version_image.tgz você não precisa extrair o arquivo ONTAP-version_image.tgz.

4. No prompt Loader, configure a conexão netboot para um LIF de gerenciamento:
   - Se o endereçamento IP for DHCP, configure a conexão automática:

     ```
     ifconfig e0M -auto
     ```

   - Se o endereçamento IP for estático, configure a conexão manual:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Execute o netboot.
   - Se a plataforma for um sistema da série 80xx, use este comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se a plataforma for qualquer outro sistema, use o seguinte comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
     ```

6. No menu de arranque, selecione a opção **(7) Instalar primeiro o novo software** para transferir e instalar a nova imagem de software no dispositivo de arranque.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se você for solicitado a continuar o procedimento, digite `y` e,
   quando solicitado a fornecer o pacote, digite o URL do arquivo de
   imagem: `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

```
Enter username/password if applicable, or press Enter to continue.
```

7. Certifique-se de entrar `n` para ignorar a recuperação de backup quando você vir um prompt semelhante ao seguinte:

```
Do you want to restore the backup configuration now? {y|n}
```

8. Reinicie entrando `y` quando você vir um prompt semelhante ao seguinte:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

Limpando a configuração em um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   `halt`

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

   `set-defaults`

3. Salvar o ambiente:

   `saveenv`

4. No prompt DO Loader, inicie o menu de inicialização:

   `boot_ontap menu`

5. No prompt do menu de inicialização, desmarque a configuração:

   `wipeconfig`

   Responda `yes` ao prompt de confirmação.

   O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

   Responda `yes` ao prompt de confirmação.

Restaurar a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:

   a. Verifique as definições atuais das portas: `ucadmin show`

   b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
Destino de FC	`fcadmin config -t target` *`adapter-name`*
Iniciador FC	`fcadmin config -t initiator` *`adapter-name`*

2. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

3. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

4. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Reatribuir discos agregados de raiz

Reatribua os discos agregados raiz ao novo módulo de controladora, usando o `sysids` recolhido anteriormente

Sobre esta tarefa

Esta tarefa é executada no modo Manutenção.

As IDs de sistema antigas foram identificadas no "Recolha de informações antes da atualização".

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Nó	ID do sistema antigo	Nova ID do sistema
node_B_1	4068741254	1574774970

Passos

1. Cable todas as outras conexões aos novos módulos de controladora (FC-VI, armazenamento, interconexão de cluster, etc.).
2. Interrompa o sistema e inicie para o modo de manutenção a partir do prompt Loader:

   ```
   boot_ontap maint
   ```

3. Exiba os discos de propriedade de node_B_1-old:

   ```
   disk show -a
   ```

   A saída do comando mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (4068741254). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   ...
   ```

4. Reatribua os discos agregados de raiz nas gavetas de unidades à nova controladora:

```
disk reassign -s old-sysid -d new-sysid
```

O exemplo a seguir mostra a reatribuição de unidades:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verifique se todos os discos estão reatribuídos conforme esperado:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK         OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Exibir o status agregado:

   `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Repita as etapas acima no nó do parceiro (node_B_2-novo).

Inicializando os novos controladores

Você deve reiniciar os controladores a partir do menu de inicialização para atualizar a imagem flash do controlador. Etapas adicionais são necessárias se a criptografia estiver configurada.

Você pode reconfigurar VLANs e grupos de interface. Se necessário, modifique manualmente as portas para os LIFs de cluster e os detalhes do domínio de broadcast antes de retomar a operação usando o `system controller replace resume` comando.

Sobre esta tarefa

Esta tarefa deve ser executada em todos os novos controladores.

Passos

1. Parar o nó:

   ```
   halt
   ```

2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Apresentar o menu de arranque:

   ```
   boot_ontap menu
   ```

4. Se a criptografia raiz for usada, selecione a opção do menu de inicialização para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

5. Se a opção autoboot estiver ativada, interrompa a operação pressionando Ctrl-C..
6. No menu de inicialização, execute a opção "'6".

   A opção "'6" reiniciará o nó duas vezes antes de concluir.

   Responda "y" aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Verifique se o parceiro-sysid está correto:

```
printenv partner-sysid
```

Se o parceiro-sysid não estiver correto, defina-o:

```
setenv partner-sysid partner-sysID
```

8. Se a criptografia raiz for usada, selecione a opção do menu de inicialização novamente para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção "'10" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

Dependendo da configuração do gerenciador de chaves, execute o procedimento de recuperação selecionando a opção ""10"" ou a opção ""11"", seguida da opção ""6"" no primeiro prompt do menu de inicialização. Para inicializar os nós completamente, você pode precisar repetir o procedimento de recuperação continuado pela opção "'1'" (inicialização normal).

9. Inicialize os nós:

```
boot_ontap
```

10. Aguarde que os nós substituídos iniciem.

Se um dos nós estiver no modo de aquisição, execute um giveback usando o `storage failover giveback` comando.

11. Verifique se todas as portas estão em um domínio de broadcast:

a. Veja os domínios de broadcast:

```
network port broadcast-domain show
```

b. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

"Adicionar ou remover portas de um domínio de broadcast"

c. Adicione a porta física que hospedará os LIFs entre clusters ao domínio de broadcast correspondente.

d. Modifique LIFs entre clusters para usar a nova porta física como porta inicial.

e. Depois que os LIFs entre clusters estiverem ativos, verifique o status de peer do cluster e restabeleça o peering de cluster conforme necessário.

Talvez seja necessário reconfigurar o peering de cluster.

"Criando um relacionamento de cluster peer"

f. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

a. Verifique se o cluster de parceiros está acessível e se a configuração é ressincronizada com êxito no cluster de parceiros:

```
metrocluster switchback -simulate true
```

12. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

13. Antes de retomar a operação, verifique se o MetroCluster está configurado corretamente. Verifique o status do nó:

```
metrocluster node show
```

Verifique se os novos nós (site_B) estão em **aguardando o estado switchback** do site_A.

14. Retomar a operação:

```
system controller replace resume
```

A concluir a atualização

A operação de automação executa verificações do sistema e, em seguida, pausa para que você possa verificar a acessibilidade da rede. Após a verificação, a fase de recuperação de recursos é iniciada e a operação de automação executa switchback no local A e pausa nas verificações pós-atualização. Depois de retomar a operação de automação, ele executa as verificações de pós-atualização e, se nenhum erro for detetado, marca a atualização como concluída.

Passos

1. Verifique a acessibilidade da rede seguindo a mensagem do console.
2. Após concluir a verificação, retome a operação:

```
system controller replace resume
```

3. A operação de automação executa switchback no local A e as verificações de atualização pós. Quando a operação for interrompida, verifique manualmente o status do SAN LIF e verifique a configuração da rede seguindo a mensagem do console.
4. Após concluir a verificação, retome a operação:

   ```
   system controller replace resume
   ```

5. Verifique o status das verificações de pós-atualização:

   ```
   system controller replace show
   ```

   Se as verificações pós-atualização não reportaram erros, a atualização está concluída.

6. Depois de concluir a atualização do controlador, inicie sessão no local B e verifique se os controladores substituídos estão configurados corretamente.

Restaurar a monitorização do desempate

Se a configuração do MetroCluster tiver sido configurada anteriormente para monitoramento pelo software tiebreaker, você poderá restaurar a conexão tiebreaker.

1. Siga as etapas em "Adição de configurações do MetroCluster".

Atualização de controladores em uma configuração IP MetroCluster usando switchover e switchback (ONTAP 9.8 e posterior)

A partir do ONTAP 9.8, você pode usar a operação de switchover do MetroCluster para fornecer serviços sem interrupções aos clientes enquanto os módulos de controladora no cluster de parceiros são atualizados. Outros componentes (como prateleiras de armazenamento ou switches) não podem ser atualizados como parte deste procedimento.

Plataformas suportadas por este procedimento

- As plataformas devem estar executando o ONTAP 9.8 ou posterior.
- A plataforma alvo (nova) deve ser um modelo diferente da plataforma original.
- Você só pode atualizar modelos de plataforma específicos usando este procedimento em uma configuração IP do MetroCluster.
  - Para obter informações sobre quais combinações de atualização de plataforma são suportadas, consulte a tabela de atualização IP do MetroCluster no "Escolha um procedimento de atualização da controladora".

```
https://docs.netapp.com/us-en/ontap-
metrocluster/upgrade/concept_choosing_controller_upgrade_mcc.html#cho
osing-a-procedure-that-uses-the-switchover-and-switchback-
process["Escolher um método de atualização ou atualização"]Consulte
para obter mais procedimentos.
```

Sobre esta tarefa

- Este procedimento aplica-se aos módulos do controlador numa configuração IP do MetroCluster.
- Todos os controladores na configuração devem ser atualizados durante o mesmo período de manutenção.

  A operação da configuração do MetroCluster com diferentes tipos de controlador não é suportada fora desta atividade de manutenção.

- Os switches IP MetroCluster (tipo de switch, fornecedor e modelo) e a versão do firmware devem ser suportados nos controladores existentes e novos na configuração de atualização.

  Consulte a "NetApp Hardware Universe"ou a "IMT" para obter informações sobre switches e versões de firmware compatíveis.

- Se estiver ativado no seu sistema, "desative a criptografia de ponta a ponta" antes de executar a atualização.
- Se a nova plataforma tiver menos slots do que o sistema original, ou se tiver menos ou diferentes tipos de portas, talvez seja necessário adicionar um adaptador ao novo sistema.
- Você reutiliza os endereços IP, as máscaras de rede e os gateways das plataformas originais nas novas plataformas.

Os seguintes nomes de exemplo são usados neste procedimento:

- Local_A
  - Antes da atualização:
    - Node_A_1-old
    - Node_A_2-old
  - Após a atualização:
    - Node_A_1-novo
    - Node_A_2-novo
- Local_B
  - Antes da atualização:
    - Node_B_1-old
    - Node_B_2-old
  - Após a atualização:
    - Node_B_1-novo
    - Node_B_2-novo

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Defina o bootarg necessário no sistema existente

Se você estiver atualizando para um sistema AFF A70, AFF A90 ou AFF A1K, siga as etapas para definir o `hw.cxgbe.toe_keepalive_disable=1` bootarg.

> Se você estiver atualizando para um sistema AFF A70, AFF A90 ou AFF A1K, **deve** concluir esta tarefa antes de executar a atualização. Esta tarefa **somente** se aplica a atualizações para um sistema AFF A70, AFF A90 ou AFF A1K a partir de um sistema suportado. Para todas as outras atualizações, você pode pular esta tarefa e ir diretamente para Prepare-se para a atualização.

Passos

1. Pare um nó em cada local e permita que seu parceiro de HA faça um takeover do nó:

   ```
   halt -node <node_name>
   ```

2. No `LOADER` prompt do nó interrompido, digite o seguinte:

   ```
   setenv hw.cxgbe.toe_keepalive_disable 1

   saveenv

   printenv hw.cxgbe.toe_keepalive_disable
   ```

3. Inicialize o nó:

   ```
   boot_ontap
   ```

4. Quando o nó for inicializado, execute um giveback para o nó no prompt:

   ```
   storage failover giveback -ofnode <node_name>
   ```

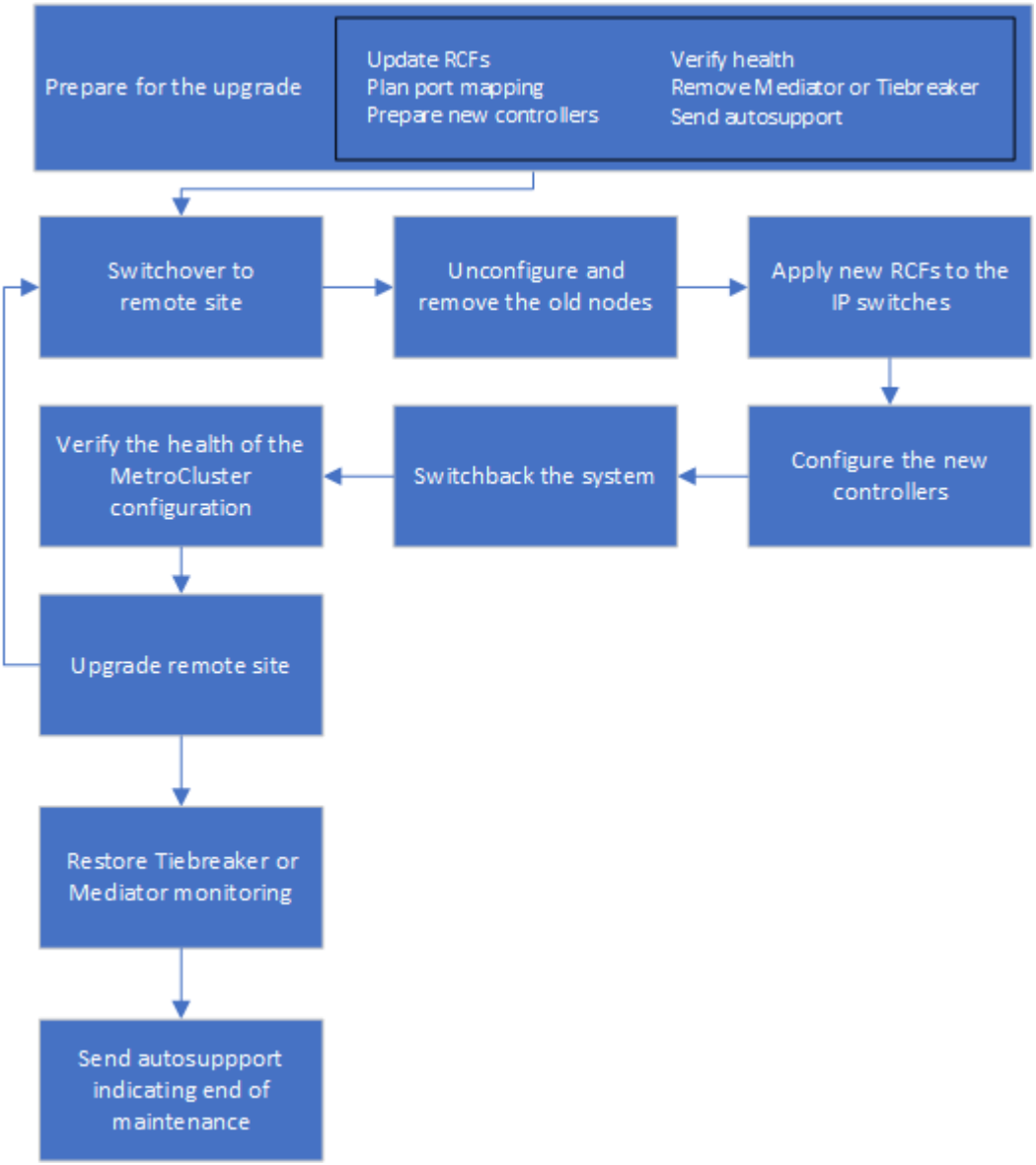
5. Repita as etapas em cada nó no grupo DR que está sendo atualizado.

Prepare-se para a atualização

Antes de fazer quaisquer alterações na configuração do MetroCluster existente, você deve verificar a integridade da configuração, preparar as novas plataformas e executar outras tarefas diversas.

Fluxo de trabalho para atualizar controladores em uma configuração IP MetroCluster

Você pode usar o diagrama de fluxo de trabalho para ajudá-lo a Planejar as tarefas de atualização.



Atualize os arquivos RCF do switch MetroCluster antes de atualizar os controladores

Dependendo dos modelos de plataforma antigos, ou se a configuração do switch não estiver na versão mínima, ou se você quiser alterar IDs de VLAN usados pelas conexões MetroCluster back-end, você deve atualizar os arquivos RCF do switch antes de iniciar o procedimento de atualização da plataforma.

Sobre esta tarefa

Você deve atualizar o arquivo RCF nos seguintes cenários:

- Para determinados modelos de plataforma, os switches devem estar usando um ID VLAN suportado para

as conexões IP MetroCluster back-end. Se os modelos de plataforma antigos ou novos estiverem na tabela a seguir, **e não** usando um ID VLAN suportado, você deverá atualizar os arquivos RCF do switch.

> As conexões de cluster locais podem usar qualquer VLAN, elas não precisam estar no intervalo especificado.

Modelo de plataforma (antigo ou novo)	IDs de VLAN suportadas
• AFF A400	• 10 • 20 • Qualquer valor no intervalo de 101 a 4096 inclusive.

- A configuração do switch não foi configurada com a versão RCF mínima suportada:

Modelo do interrutor	Versão necessária do ficheiro RCF
Cisco 3132Q-V	1,7 ou posterior
Cisco 3232C	1,7 ou posterior
Broadcom BES-53248	1,3 ou posterior

- Você deseja alterar a configuração da VLAN.

  O intervalo de ID de VLAN é de 101 a 4096 inclusive.

Os switches no site_A serão atualizados quando os controladores no site_A forem atualizados.

Passos

1. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"
2. Baixe e instale os arquivos RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Baixe e instale os arquivos Broadcom RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

Mapear portas dos nós antigos para os novos nós

Você deve verificar se as portas físicas no node_A_1-old mapeiam corretamente para as portas físicas no

node_A_1-novo, o que permitirá que node_A_1-novo se comunique com outros nós no cluster e com a rede após a atualização.

Sobre esta tarefa

Quando o novo nó é inicializado pela primeira vez durante o processo de atualização, ele reproduzirá a configuração mais recente do nó antigo que está substituindo. Quando você inicializa node_A_1-novo, o ONTAP tenta hospedar LIFs nas mesmas portas que foram usadas no node_A_1-old. Portanto, como parte da atualização, você deve ajustar a configuração de porta e LIF para que seja compatível com a do nó antigo. Durante o procedimento de atualização, você executará etapas nos nós antigos e novos para garantir a configuração correta de cluster, gerenciamento e LIF de dados.

A tabela a seguir mostra exemplos de alterações de configuração relacionadas aos requisitos de porta dos novos nós.

Portas físicas de interconexão de cluster		
Controlador antigo	Novo controlador	Ação necessária
e0a, e0b	e3a, e3b	Nenhuma porta correspondente. Após a atualização, você deve recriar as portas do cluster.
e0c, e0d	e0a, e0b, e0c, e0d	e0c e e0d são portas correspondentes. Você não precisa alterar a configuração, mas após a atualização, você pode espalhar suas LIFs de cluster pelas portas de cluster disponíveis.

Passos

1. Determine quais portas físicas estão disponíveis nos novos controladores e quais LIFs podem ser hospedados nas portas.

   O uso da porta do controlador depende do módulo da plataforma e quais switches você usará na configuração IP do MetroCluster. Você pode coletar o uso de portas das novas plataformas do "NetApp Hardware Universe".

2. Planeje o uso da porta e preencha as tabelas a seguir para referência para cada um dos novos nós.

   Irá consultar a tabela à medida que realizar o procedimento de atualização.

	Node_A_1-old			Node_A_1-novo		
LIF	Portas	IPspaces	Domínios de broadcast	Portas	IPspaces	Domínios de broadcast
Cluster 1						
Cluster 2						
Cluster 3						

Cluster 4						
Gerenciamento de nós						
Gerenciamento de clusters						
Dados 1						
Dados 2						
Dados 3						
Dados 4						
SAN						
Porta entre clusters						

Netboot os novos controladores

Depois de instalar os novos nós, você precisa netboot para garantir que os novos nós estejam executando a mesma versão do ONTAP que os nós originais. O termo netboot significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para netboot, você deve colocar uma cópia da imagem de inicialização do ONTAP 9 em um servidor da Web que o sistema possa acessar.

Passos

1. Netboot os novos controladores:

   a. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.

   b. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o `ontap-version_image.tgz` ficheiro num diretório acessível pela Web.

   c. Mude para o diretório acessível pela Web e verifique se os arquivos necessários estão disponíveis.

      Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel:

      `_ontap-version_image.tgz`

      Você não precisa extrair o `_ontap-version_image.tgz` arquivo.

   d. No prompt Loader, configure a conexão netboot para um LIF de gerenciamento:

Se o endereço IP for…	Então…

DHCP	Configurar a ligação automática: `ifconfig e0M -auto`
Estático	Configurar a ligação manual: `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

e. Execute o netboot.

```
netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
```

f. No menu de inicialização, selecione a opção **(7) instale primeiro o novo software** para baixar e instalar a nova imagem de software no dispositivo de inicialização.

Ignore a seguinte mensagem:

`"This procedure is not supported for Non-Disruptive Upgrade on an HA pair"`. Isso se aplica a atualizações de software sem interrupções, e não a atualizações de controladores.

a. Se você for solicitado a continuar o procedimento, digite `y` e, quando solicitado a fornecer o pacote, digite o URL do arquivo de imagem:

`http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

b. Introduza o nome de utilizador e a palavra-passe, se aplicável, ou prima Enter para continuar.

c. Certifique-se de entrar `n` para ignorar a recuperação de backup quando você vir um prompt semelhante ao seguinte:

```
Do you want to restore the backup configuration now? {y|n} n
```

d. Reinicie entrando **`y`** quando você vir um prompt semelhante ao seguinte:

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
```

Limpe a configuração de um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

```
halt
```

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

```
set-defaults
```

3. Salvar o ambiente:

```
saveenv
```

4. No prompt DO Loader, inicie o menu de inicialização:

```
boot_ontap menu
```

5. No prompt do menu de inicialização, desmarque a configuração:

```
wipeconfig
```

Responda `yes` ao prompt de confirmação.

O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

Responda `yes` ao prompt de confirmação.

Verifique a integridade do MetroCluster antes da atualização do site

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a atualização.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:

   a. Verifique se os nós são multipathed: Mais
   `node run -node <node_name> sysconfig -a`

   Você deve emitir este comando para cada nó na configuração do MetroCluster.

   b. Verifique se não há discos quebrados na configuração
   `storage disk show -broken`

   Você deve emitir este comando em cada nó na configuração do MetroCluster.

   c. Verifique se existem alertas de saúde:

   ```
   system health alert show
   ```

   Você deve emitir este comando em cada cluster.

   d. Verifique as licenças nos clusters:

   ```
   system license show
   ```

Você deve emitir este comando em cada cluster.

e. Verifique os dispositivos conetados aos nós:

```
network device-discovery show
```

Você deve emitir este comando em cada cluster.

f. Verifique se o fuso horário e a hora estão definidos corretamente em ambos os sites:

```
cluster date show
```

Você deve emitir este comando em cada cluster. Pode utilizar os `cluster date` comandos para configurar a hora e o fuso horário.

2. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional é `normal`
   `metrocluster show`
   b. Confirme que todos os nós esperados são mostrados
   `metrocluster node show`
   c. Emita o seguinte comando:

```
metrocluster check run
```

   d. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

3. Verifique o cabeamento do MetroCluster com a ferramenta Config Advisor.
   a. Baixe e execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

   b. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Reúna informações antes da atualização

Antes de atualizar, você deve reunir informações para cada um dos nós e, se necessário, ajustar os domínios de broadcast de rede, remover quaisquer VLANs e grupos de interfaces e reunir informações de criptografia.

Passos

1. Registre o cabeamento físico de cada nó, rotulando os cabos conforme necessário para permitir o cabeamento correto dos novos nós.
2. Reunir informações de interconexão, porta e LIF para cada nó.

   Você deve reunir a saída dos seguintes comandos para cada nó:

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`

- `network interface show -role cluster,node-mgmt`
- `network port show -node <node_name> -type physical`
- `network port vlan show -node <node_name>`
- `network port ifgrp show -node <node_name> -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node <node_name> sysconfig -a`
- `aggr show -r`
- `disk show`
- `system node run <node-name> disk show`
- `vol show -fields type`
- `vol show -fields type , space-guarantee`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

3. Reúna os UUIDs para o site_B (o site cujas plataformas estão sendo atualizadas):

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Esses valores devem ser configurados com precisão nos novos módulos do controlador site_B para garantir uma atualização bem-sucedida. Copie os valores para um arquivo para que você possa copiá-los para os comandos apropriados posteriormente no processo de atualização.

   O exemplo a seguir mostra a saída do comando com os UUIDs:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

É recomendável que você grave os UUIDs em uma tabela semelhante à seguinte.

Cluster ou nó	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	a9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves:

   `security key-manager backup show`

6. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações sobre as chaves e senhas.

   Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

   a. Se o Gerenciador de chaves integrado estiver configurado
   `security key-manager onboard show-backup`

      Você precisará da senha mais tarde no procedimento de atualização.

   b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

   ```
   security key-manager external show -instance
   security key-manager key query
   ```

7. Reúna as IDs do sistema dos nós existentes:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   A saída a seguir mostra as unidades reatribuídas.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
-------------------- ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Remova a monitorização do Mediator ou do tiebreaker

Antes de atualizar as plataformas, você deve remover o monitoramento se a configuração do MetroCluster for monitorada com o utilitário tiebreaker ou Mediator.

Passos

1. Colete a saída para o seguinte comando:

```
storage iscsi-initiator show
```

2. Remova a configuração do MetroCluster existente do tiebreaker, Mediator ou outro software que possa iniciar o switchover.

Se você estiver usando…	Use este procedimento…
Desempate	"Remoção das configurações do MetroCluster"
Mediador	Execute o seguinte comando no prompt do ONTAP: `metrocluster configuration-settings mediator remove`
Aplicativos de terceiros	Consulte a documentação do produto.

Envie uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Inicie sessão no cluster.
2. Chame uma mensagem AutoSupport indicando o início da manutenção:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   O `maintenance-window-in-hours` parâmetro especifica o comprimento da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Repita estas etapas no site do parceiro.

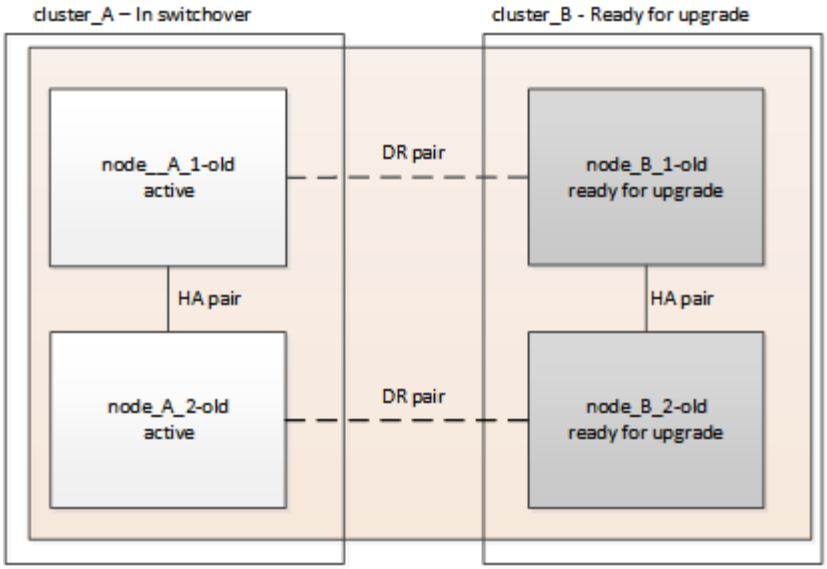
Alterne a configuração do MetroCluster

Você deve alternar a configuração para site_A para que as plataformas no site_B possam ser atualizadas.

Sobre esta tarefa

Esta tarefa tem de ser executada no site_A.

Depois de concluir esta tarefa, o cluster_A está ativo e fornecendo dados para ambos os sites. O cluster_B está inativo e pronto para iniciar o processo de atualização.



Passos

1. Alterne a configuração do MetroCluster para site_A para que os nós do site_B possam ser atualizados:

   a. Execute o seguinte comando no cluster_A:

      `metrocluster switchover -controller-replacement true`

      A operação pode levar vários minutos para ser concluída.

   b. Monitorize a operação de comutação:

      `metrocluster operation show`

   c. Após a conclusão da operação, confirme se os nós estão no estado de comutação:

      `metrocluster show`

   d. Verifique o status dos nós MetroCluster:

      `metrocluster node show`

   A recuperação automática de agregados após o switchover negociado é desativada durante a atualização do controlador.

Remova as configurações de interface e desinstale os controladores antigos

Verifique a colocação correta de LIF. Em seguida, remova as VLANs e os grupos de interface nos controladores antigos e desinstale fisicamente os controladores.

Sobre esta tarefa

- Essas etapas são executadas nos controladores antigos (node_B_1-old, node_B_2-old).
- Consulte as informações coletadas no "Mapear portas dos nós antigos para os novos nós".

Passos

1. Inicialize os nós antigos e faça login nos nós:

```
boot_ontap
```

2. Modifique as LIFs entre clusters nos controladores antigos para usar uma porta inicial diferente das portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nos novos controladores.

   Esta etapa é necessária para uma atualização bem-sucedida.

   As LIFs entre clusters nos controladores antigos devem usar uma porta inicial diferente das portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nos novos controladores. Por exemplo, quando você faz upgrade para controladoras AFF A90, as portas de interconexão de HA são e1a e e7a e as portas de interconexão de DR IP MetroCluster são E2B e e3b. Você deve mover as LIFs entre clusters nos controladores antigos se eles estiverem hospedados nas portas e1a, e7a, E2B ou e3b.

   Para a distribuição e alocação de portas nos novos nós, consulte o "NetApp Hardware Universe".

   a. Nos controladores antigos, veja os LIFs entre clusters:

      ```
      network interface show -role intercluster
      ```

      Execute uma das ações a seguir, dependendo se as LIFs entre clusters nos controladores antigos usam as mesmas portas que as portas usadas para interconexão de HA ou interconexão de DR IP MetroCluster nas novas controladoras.

Se os LIFs entre clusters…	**Ir para…**
Use a mesma porta inicial	Subpasso b
Utilize uma porta inicial diferente	Passo 3

   b. modifique os LIFs entre clusters para usar uma porta inicial diferente:

      ```
      network interface modify -vserver <vserver> -lif <intercluster_lif> -home
      -port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-
      nodes>
      ```

   c. Verifique se todas as LIFs entre clusters estão em suas novas portas residenciais:

      ```
      network interface show -role intercluster -is-home false
      ```

      A saída do comando deve estar vazia, indicando que todas as LIFs entre clusters estão em suas respetivas portas residenciais.

   d. Se houver LIFs que não estejam em suas portas residenciais, reverta-os usando o seguinte comando:

      ```
      network interface revert -lif <intercluster_lif>
      ```

   Repita o comando para cada LIF entre clusters que não está na porta inicial.

3. atribua a porta inicial de todos os LIFs de dados no controlador antigo a uma porta comum que é a mesma nos módulos de controladora antigos e novos.

   Se os controladores antigos e novos não tiverem uma porta comum, não será necessário modificar as LIFs de dados. Pule esta etapa e vá diretamente para Passo 4.

a. Apresentar os LIFs:

```
network interface show
```

Todos os LIFS de dados, incluindo SAN e nas, serão administradores acima e operacionalmente inativos, uma vez que eles estão ativos no local de switchover (cluster_A).

b. Revise a saída para encontrar uma porta de rede física comum que seja a mesma nos controladores antigos e novos que não seja usada como uma porta de cluster.

Por exemplo, e0d é uma porta física em controladores antigos e também está presente em novos controladores. e0d não é usado como uma porta de cluster ou de outra forma nos novos controladores.

Para obter informações sobre a utilização de portas para modelos de plataforma, consulte a. "NetApp Hardware Universe"

c. Modifique todos os dados LIFS para usar a porta comum como a porta inicial
`network interface modify -vserver <svm-name> -lif <data-lif> -home-port <port-id>`

No exemplo a seguir, isso é "e0d".

Por exemplo:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

4. Modificar domínios de broadcast para remover a VLAN e as portas físicas que precisam ser excluídas:

```
broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name> -ports <node-name:port-id>
```

Repita esta etapa para todas as portas VLAN e físicas.

5. Remova quaisquer portas VLAN usando portas de cluster como portas membro e ifgrps usando portas de cluster como portas membro.

a. Excluir portas VLAN
`network port vlan delete -node <node_name> -vlan-name <portid-vlandid>`

Por exemplo:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remover portas físicas dos grupos de interface:

```
network port ifgrp remove-port -node <node_name> -ifgrp <interface-group-name> -port <portid>
```

Por exemplo:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Remova as portas VLAN e grupo de interfaces do domínio de broadcast:

```
network port broadcast-domain remove-ports -ipspace <ipspace> -broadcast
-domain <broadcast-domain-name> -ports
<nodename:portname,nodename:portnamee>,..
```

b. Modifique as portas do grupo de interfaces para usar outras portas físicas como membro, conforme necessário:

```
ifgrp add-port -node <node_name> -ifgrp <interface-group-name> -port <port-
id>
```

6. Interrompa os nós para o prompt DO Loader:

```
halt -inhibit-takeover true
```

7. Conete-se ao console serial dos controladores antigos (node_B_1-old e node_B_2-old) no site_B e verifique se ele está exibindo o prompt Loader.
8. Reúna os valores do bootarg:

```
printenv
```

9. Desconete as conexões de storage e rede em node_B_1-old e node_B_2-old e rotule os cabos para que possam ser reconetados aos novos nós.
10. Desconete os cabos de alimentação do node_B_1-old e node_B_2-old.
11. Remova os controladores node_B_1-old e node_B_2-old do rack.

Configure os novos controladores

É necessário colocar em rack e cabo as novas controladoras.

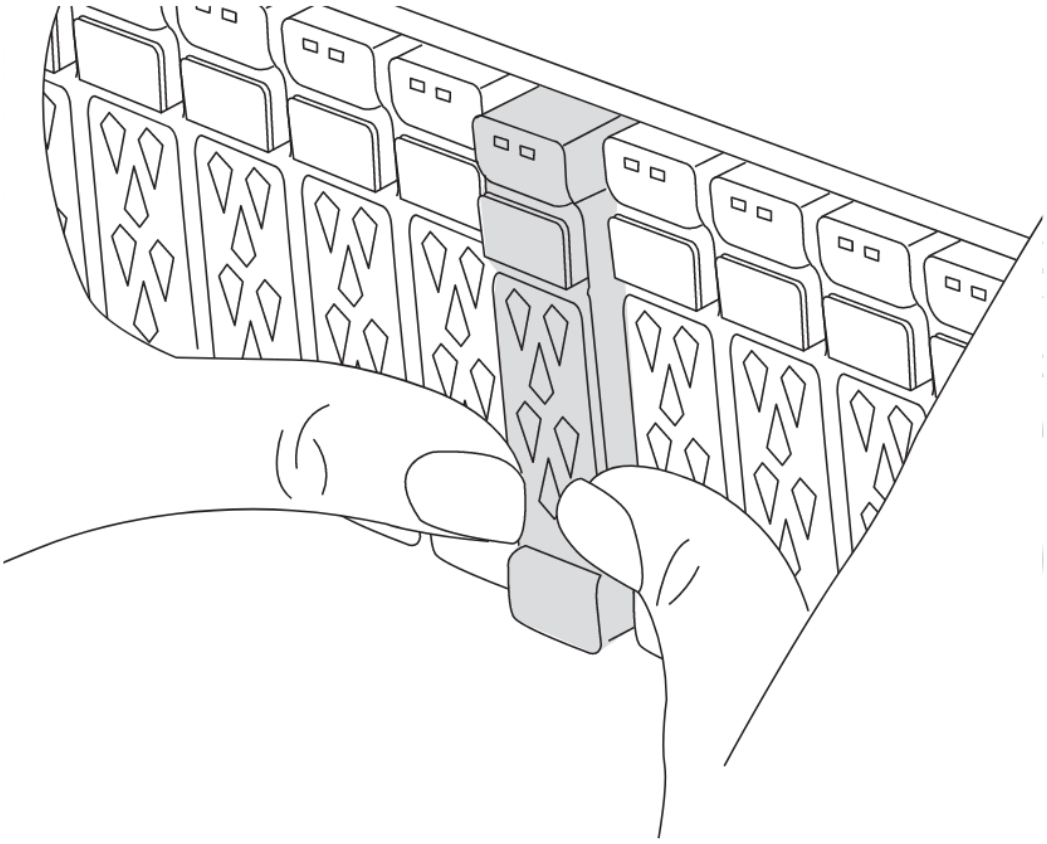
Passos

1. Planeje o posicionamento dos novos módulos de controladora e compartimentos de armazenamento conforme necessário.

   O espaço em rack depende do modelo de plataforma dos módulos de controladora, dos tipos de switch e do número de compartimentos de storage em sua configuração.

2. Aterre-se corretamente.
3. Se a atualização exigir a substituição dos módulos da controladora, por exemplo, a atualização de um sistema AFF 800 para um sistema AFF A90, você deve remover o módulo da controladora do chassi quando substituir o módulo da controladora. Para todas as outras atualizações, vá para Passo 4.

   Na parte frontal do chassis, utilize os polegares para empurrar firmemente cada unidade até sentir um batente positivo. Isto confirma que as unidades estão firmemente assentadas contra o plano médio do chassis.



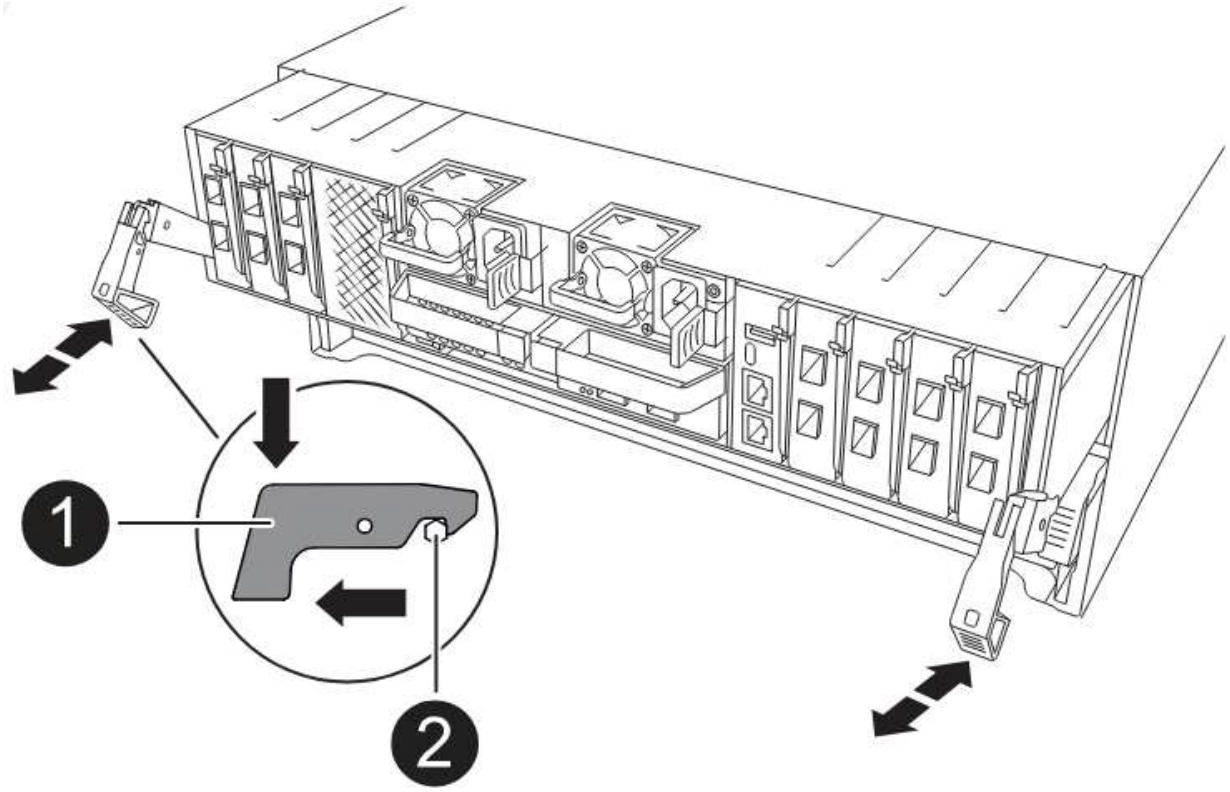
4. instale os módulos do controlador.

As etapas de instalação que você seguir dependem se a atualização requer a substituição dos módulos da controladora, como uma atualização de um sistema AFF 800 para um sistema AFF A90.

Substituição dos módulos do controlador

A instalação dos novos controladores separadamente não se aplica a atualizações de sistemas integrados com discos e controladores no mesmo chassi, por exemplo, de um sistema AFF A800 para um sistema AFF A90. Os novos módulos do controlador e as placas de e/S devem ser trocados após desligar os controladores antigos, como mostrado na imagem abaixo.

A imagem de exemplo a seguir é apenas para representação, os módulos do controlador e as placas de e/S podem variar entre sistemas.



Todas as outras atualizações

Instale os módulos do controlador no rack ou gabinete.

5. Faça o cabeamento das conexões de alimentação, console serial e gerenciamento dos controladores, conforme descrito em "Cabeamento dos switches IP MetroCluster"

   Não conete nenhum outro cabo que tenha sido desconetado dos controladores antigos neste momento.

   "Documentação dos sistemas de hardware da ONTAP"

6. Ligue os novos nós e inicialize-os no modo Manutenção.

Restaure a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:

a. Verifique as definições atuais das portas:

```
ucadmin show
```

b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…
CNA FC	`ucadmin modify -m fc -t initiator <adapter-name>`
CNA Ethernet	`ucadmin modify -mode cna <adapter-name>`
Destino de FC	`fcadmin config -t target <adapter-name>`
Iniciador FC	`fcadmin config -t initiator <adapter-name>`

2. Sair do modo de manutenção:

```
halt
```

Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

3. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

```
boot_ontap maint
```

4. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Defina o estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

```
ha-config show
```

O estado HA para todos os componentes deve ser `mccip`.

2. Se o estado do sistema apresentado do controlador ou do chassis não estiver correto, defina o estado HA:

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

3. Verifique e modifique as portas Ethernet conetadas a gavetas NS224 ou switches de storage.

   a. Verifique as portas Ethernet conetadas a gavetas NS224 ou switches de armazenamento:

      `storage port show`

   b. Defina todas as portas Ethernet conetadas a gavetas Ethernet ou switches de armazenamento, incluindo switches compartilhados para armazenamento e cluster, para o `storage` modo:

      `storage port modify -p <port> -m storage`

      Exemplo:

      ```
      *> storage port modify -p e5b -m storage
      Changing NVMe-oF port e5b to storage mode
      ```

      Isso deve ser definido em todas as portas afetadas para uma atualização bem-sucedida.

      Os discos das gavetas conetadas às portas Ethernet são reportados `sysconfig -v` na saída.

   Consulte a "NetApp Hardware Universe" para obter informações sobre as portas de armazenamento para o sistema para o qual está a atualizar.

   a. Verifique se `storage` o modo está definido e confirme se as portas estão no estado online:

      `storage port show`

4. Parar o nó: `halt`

   O nó deve parar no `LOADER>` prompt.

5. Em cada nó, verifique a data, a hora e o fuso horário do sistema: `show date`
6. Se necessário, defina a data em UTC ou GMT: `set date <mm/dd/yyyy>`
7. Verifique a hora usando o seguinte comando no prompt do ambiente de inicialização: `show time`
8. Se necessário, defina a hora em UTC ou GMT: `set time <hh:mm:ss>`
9. Guarde as definições: `saveenv`
10. Reunir variáveis de ambiente: `printenv`

Atualize os RCFs do switch para acomodar as novas plataformas

Você deve atualizar os switches para uma configuração que suporte os novos modelos de plataforma.

Sobre esta tarefa

Você executa essa tarefa no site que contém os controladores que estão sendo atualizados no momento. Nos exemplos mostrados neste procedimento, estamos atualizando site_B primeiro.

Os switches no site_A serão atualizados quando os controladores no site_A forem atualizados.

Passos

1. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas do procedimento para o fornecedor do switch:

   "Instalação e configuração IP do MetroCluster"

   - "[Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"

2. Baixe e instale os arquivos RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Baixe e instale os arquivos Broadcom RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros RCF switch IP SN2100 da NVIDIA"

Defina as variáveis MetroCluster IP bootarg

Certos valores de inicialização IP do MetroCluster devem ser configurados nos novos módulos do controlador. Os valores devem corresponder aos configurados nos módulos do controlador antigos.

Sobre esta tarefa

- Você precisa dos UUIDs e IDs de sistema identificados anteriormente no procedimento de atualização no Reúna informações antes da atualização.
- Dependendo do modelo da plataforma, você pode especificar o ID da VLAN usando o `-vlan-id` parâmetro. As seguintes plataformas não suportam o `-vlan-id` parâmetro:
  - FAS8200 e AFF A300
  - AFF A320
  - FAS9000 e AFF A700
  - AFF C800, ASA C800, AFF A800 e ASA A800

    Todas as outras plataformas suportam o `-vlan-id` parâmetro.

- Os valores de bootarg do MetroCluster definidos dependem se o novo sistema utiliza portas de cluster/HA partilhadas ou portas MetroCluster/HA partilhadas.

  Os sistemas listados na tabela a seguir usam **portas MetroCluster/HA compartilhadas**.

  Todos os outros sistemas usam **portas de cluster/HA compartilhadas**.

Sistemas AFF e ASA usando portas MetroCluster/HA compartilhadas	Sistemas FAS que usam portas MetroCluster/HA compartilhadas
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

Passos

1. `LOADER>`No prompt, defina os seguintes bootargs nos novos nós no site_B:

   As etapas a seguir dependem das portas usadas pelo novo modelo de plataforma.

Sistemas que usam portas de cluster/HA compartilhadas

a. Defina os seguintes bootargs:

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id>
```

> Se as interfaces estiverem usando um ID de VLAN padrão, o `vlan-id` parâmetro não será necessário.

O exemplo a seguir define os valores para node_B_1-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir define os valores para node_B_2-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13,130
```

O exemplo a seguir define os valores para node_B_1-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

O exemplo a seguir define os valores para node_B_2-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,0,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,0,172.17.27.12,172.17.27.13
```

Sistemas que usam portas MetroCluster/HA compartilhadas

a. Defina os seguintes bootargs:

```
setenv bootarg.mcc.port_a_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>

setenv bootarg.mcc.port_b_ip_config <local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id>
```

> Se as interfaces estiverem usando um ID de VLAN padrão, o `vlan-id` parâmetro não será necessário.

O exemplo a seguir define os valores para node_B_1-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir define os valores para node_B_2-novo usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

O exemplo a seguir define os valores para node_B_1-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

O exemplo a seguir define os valores para node_B_2-novo usando VLANs padrão para todas as conexões de DR IP MetroCluster:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. No prompt Loader dos novos nós, defina os UUIDs:

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

   a. Defina os UUIDs em node_B_1-novo.

      O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_1-novo:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. Defina os UUIDs em node_B_2-novo:

      O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_2-novo:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Determine se os sistemas originais foram configurados para o Advanced Drive Partitioning (ADP) executando o seguinte comando a partir do site que está ativo:

`disk show`

A coluna "container type" (tipo de contentor) apresenta "shared" (partilhado `disk show`) na saída se o ADP estiver configurado. Se o "tipo de contentor" tiver qualquer outro valor, o ADP não está configurado no sistema. A saída de exemplo a seguir mostra um sistema configurado com ADP:

```
::> disk show
                    Usable               Disk    Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner

Info: This cluster has partitioned disks. To get a complete list of
spare disk
      capacity use "storage aggregate show-spare-disks".
----------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

4. Se os sistemas originais foram configurados com discos particionados para ADP, ative-o `LOADER` no prompt para cada nó de substituição:

   `setenv bootarg.mcc.adp_enabled true`

5. Defina as seguintes variáveis:

   `setenv bootarg.mcc.local_config_id <original-sys-id>`

   `setenv bootarg.mcc.dr_partner <dr-partner-sys-id>`

   > A `setenv bootarg.mcc.local_config_id` variável deve ser definida como o sys-id do módulo controlador **original**, node_B_1-old.

   a. Defina as variáveis em node_B_1-novo.

      O exemplo a seguir mostra os comandos para definir os valores em node_B_1-novo:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Defina as variáveis em node_B_2-novo.

      O exemplo a seguir mostra os comandos para definir os valores em node_B_2-novo:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Se estiver usando criptografia com gerenciador de chaves externo, defina os bootargs necessários:

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Reatribuir discos agregados de raiz

Reatribua os discos agregados de raiz ao novo módulo de controladora, usando os sysids reunidos anteriormente.

Sobre esta tarefa

Estes passos são executados no modo de manutenção.

> Os discos agregados de raiz são os únicos discos que devem ser reatribuídos durante o processo de atualização da controladora. A propriedade de disco de agregados de dados é tratada como parte da operação de comutação/switchback.

Passos

1. Inicialize o sistema no modo de manutenção:

```
boot_ontap maint
```

2. Exiba os discos no node_B_1-novo no prompt do modo de manutenção:

```
disk show -a
```

> Antes de prosseguir com a reatribuição de disco, você deve verificar se os discos pool0 e pool1 pertencentes ao agregado raiz do nó são exibidos na `disk show` saída. No exemplo a seguir, a saída lista os discos pool0 e pool1 de propriedade do node_B_1-old.

A saída do comando mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (537403322). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------              -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.
```

3. Reatribua os discos agregados de raiz nos compartimentos de unidades às novas controladoras.

Se você estiver usando ADP…	Em seguida, use este comando…
Sim	`disk reassign -s <old-sysid> -d <new-sysid> -r <dr-partner-sysid>`
Não	`disk reassign -s <old-sysid> -d <new-sysid>`

4. Reatribua os discos agregados de raiz nos compartimentos de unidades às novas controladoras:

   `disk reassign -s <old-sysid> -d <new-sysid>`

   O exemplo a seguir mostra a reatribuição de unidades em uma configuração não ADP:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verifique se os discos do agregado raiz estão corretamente reatribuídos à remoção antiga:

   ```
   disk show

   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Inicialize os novos controladores

Você deve inicializar os novos controladores, tomando cuidado para garantir que as variáveis bootarg estão corretas e, se necessário, executar as etapas de recuperação de criptografia.

Passos

1. Parar os novos nós:

   ```
   halt
   ```

2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

   ```
   setenv bootarg.kmip.init.ipaddr <ip-address>

   setenv bootarg.kmip.init.netmask <netmask>

   setenv bootarg.kmip.init.gateway <gateway-addres>
   ```

```
setenv bootarg.kmip.init.interface <interface-id>
```

3. Verifique se o parceiro-sysid é o atual:

   ```
   printenv partner-sysid
   ```

   Se o parceiro-sysid não estiver correto, defina-o:

   ```
   setenv partner-sysid <partner-sysID>
   ```

4. Exiba o menu de inicialização do ONTAP:

   ```
   boot_ontap menu
   ```

5. Se a criptografia raiz for usada, selecione a opção do menu de inicialização para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção `10` Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção `11` Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

6. No menu de inicialização, selecione "'(6) Atualizar flash a partir da configuração de backup".

   A opção 6 reiniciará o nó duas vezes antes de concluir.

   Responda "y" aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. NO Loader, verifique novamente os valores do bootarg e atualize os valores conforme necessário.

   Siga as etapas em "Configurando as variáveis de inicialização IP do MetroCluster".

8. Verifique se o parceiro-sysid está correto:

   ```
   printenv partner-sysid
   ```

   Se o parceiro-sysid não estiver correto, defina-o:

```
setenv partner-sysid <partner-sysID>
```

9. Se a criptografia raiz for usada, selecione a opção do menu de inicialização novamente para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção `10` Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.
Gerenciamento de chaves externas	Opção "'11" Siga as instruções para fornecer as entradas necessárias para recuperar e restaurar a configuração do gerenciador de chaves.

Dependendo da configuração do gerenciador de chaves, execute o procedimento de recuperação selecionando a opção ""10"" ou a opção ""11"", seguida da opção `6` no primeiro prompt do menu de inicialização. Para inicializar os nós completamente, você pode precisar repetir o procedimento de recuperação continuado pela opção "'1'" (inicialização normal).

10. Aguarde que os nós substituídos iniciem.

Se um dos nós estiver no modo de aquisição, execute um giveback usando o `storage failover giveback` comando.

11. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver <SVM> -node <node> -key-server <host_name`

12. Verifique se todas as portas estão em um domínio de broadcast:

a. Veja os domínios de broadcast:

```
network port broadcast-domain show
```

b. Se um novo domínio de broadcast for criado para as portas de dados nos controladores recém-atualizados, exclua o domínio de broadcast:

Exclua apenas o novo domínio de broadcast. Não exclua nenhum dos domínios de broadcast que existiam antes de iniciar a atualização.

```
broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

c. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

"Adicionar ou remover portas de um domínio de broadcast"

d. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

Verifique e restaure a configuração do LIF

Verifique se os LIFs estão hospedados em nós e portas apropriados, conforme mapeados no início do procedimento de atualização.

Sobre esta tarefa

- Esta tarefa é executada no site_B.
- Consulte o plano de mapeamento de portas criado no "Mapeamento de portas dos nós antigos para os novos nós".

Você deve verificar se o local das LIFs de dados está correto nos novos nós antes de executar um switchback. Quando você alterna a configuração, o ONTAP tenta retomar o tráfego na porta inicial usada pelos LIFs. A falha de e/S pode ocorrer quando a conexão da porta inicial com a porta do switch e VLAN estiver incorreta.

Passos

1. Verifique se os LIFs estão hospedados no nó e portas apropriados antes do switchback.

a. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

b. Exiba os LIFs e confirme se cada data LIF está usando a porta inicial correta:

```
network interface show
```

c. Modifique quaisquer LIFs que não estejam usando a porta inicial correta:

```
network interface modify -vserver <svm-name> -lif <data-lif> -home-port
<port-id>
```

Se o comando retornar um erro, você pode substituir a configuração da porta:

```
vserver config override -command "network interface modify -vserver <svm-
name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
```

```
<new_node_name>"
```

Ao entrar no comando Network Interface Modify dentro `vserver config override` do comando, não é possível usar o recurso Tab Autocomplete. Você pode criar a rede `interface modify` usando o autocomplete e, em seguida, incorporá-la no `vserver config override` comando.

a. Confirme se todas as LIFs de dados estão agora na porta inicial correta:

```
network interface show
```

b. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

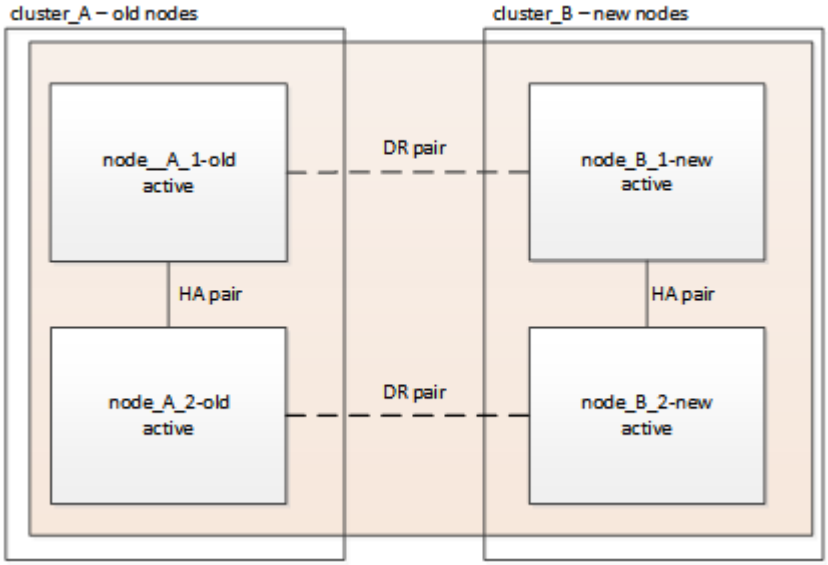
2. Reverter as interfaces para o seu nó inicial:

```
network interface revert * -vserver <svm-name>
```

Execute esta etapa em todas as SVMs, conforme necessário.

Volte a ativar a configuração do MetroCluster

Nesta tarefa, você executará a operação de switchback e a configuração do MetroCluster retornará à operação normal. Os nós no site_A ainda estão aguardando atualização.



Passos

1. Emita o `metrocluster node show` comando no site_B e verifique a saída.
   a. Verifique se os novos nós estão representados corretamente.
   b. Verifique se os novos nós estão em "aguardando pelo estado de switchback".
2. Execute a recuperação e o switchback executando os comandos necessários de qualquer nó no cluster ativo (o cluster que não está sendo atualizado).
   a. Curar os agregados de dados
   `metrocluster heal aggregates`

b. Curar os agregados de raiz:

```
metrocluster heal root
```

c. Comutar o cluster:

```
metrocluster switchback
```

3. Verifique o progresso do funcionamento do interrutor de comutação:

```
metrocluster show
```

A operação de switchback ainda está em andamento quando a saída exibe `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

A operação de comutação está concluída quando a saída exibe normal:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o `metrocluster config-replication resync-status show` comando. Este comando está no nível de privilégio avançado.

Verifique a integridade da configuração do MetroCluster

Depois de atualizar os módulos do controlador, você deve verificar a integridade da configuração do MetroCluster.

Sobre esta tarefa

Esta tarefa pode ser executada em qualquer nó na configuração do MetroCluster.

Passos

1. Verifique o funcionamento da configuração do MetroCluster:
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal
   `metrocluster show`
   b. Execute uma verificação MetroCluster
   `metrocluster check run`
   c. Apresentar os resultados da verificação MetroCluster:

   ```
   metrocluster check show
   ```

2. Verifique a conetividade e o status do MetroCluster.
   a. Verifique as conexões IP do MetroCluster:

   ```
   storage iscsi-initiator show
   ```

   b. Verifique se os nós estão operando:

   ```
   metrocluster node show
   ```

   c. Verifique se as interfaces IP do MetroCluster estão ativas:

   ```
   metrocluster configuration-settings interface show
   ```

   d. Verifique se o failover local está ativado:

   ```
   storage failover show
   ```

Atualize os nós no cluster_A

Você deve repetir as tarefas de atualização no cluster_A.

Passos

1. Repita as etapas para atualizar os nós no cluster_A, começando com "Preparando-se para a atualização".

   À medida que você executa as tarefas, todas as referências de exemplo aos clusters e nós são invertidas. Por exemplo, quando o exemplo é dado para o switchover de cluster_A, você irá mudar de cluster_B.

Restaure o monitoramento do tiebreaker ou do Mediator

Depois de concluir a atualização da configuração do MetroCluster, você pode retomar o monitoramento com o utilitário tiebreaker ou Mediator.

Passos

1. Restaure o monitoramento, se necessário, usando o procedimento para sua configuração.

Se você estiver usando…	Use este procedimento
Desempate	"Adição de configurações do MetroCluster".

Se você estiver usando…	Use este procedimento
Mediador	"Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster".
Aplicativos de terceiros	Consulte a documentação do produto.

Envie uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a atualização, você deve enviar uma mensagem AutoSupport indicando o fim da manutenção, para que a criação automática de casos possa ser retomada.

Passos

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.
   a. Execute o seguinte comando
   `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repita o comando no cluster de parceiros.

Configurar criptografia de ponta a ponta

Se for compatível com o sistema, você poderá criptografar o tráfego de back-end, como NVlog e dados de replicação de armazenamento, entre os sites IP do MetroCluster. "Configurar criptografia de ponta a ponta"Consulte para obter mais informações.

Atualizar controladores de AFF A700/FAS9000 para AFF A900/FAS9500 em uma configuração IP MetroCluster usando switchover e switchback (ONTAP 9.10,1 ou posterior)

Você pode usar a operação switchover do MetroCluster para fornecer serviços sem interrupções aos clientes enquanto os módulos de controladora no cluster de parceiros são atualizados. Outros componentes (como prateleiras de armazenamento ou switches) não podem ser atualizados como parte deste procedimento.

Sobre esta tarefa

- Para atualizar os módulos do controlador AFF A700 para o AFF A900, os controladores devem estar executando o ONTAP 9.10,1 ou posterior.
- Para atualizar os módulos do controlador FAS9000 para o FAS9500, os controladores devem estar executando o ONTAP 9.10.1P3 ou posterior.
- Todos os controladores na configuração devem ser atualizados durante o mesmo período de manutenção.

  Operar a configuração do MetroCluster com um AFF A700 e um AFF A900, ou um controlador FAS9000 e um FAS9500 não é suportado fora desta atividade de manutenção.

- Os switches IP devem estar executando uma versão de firmware suportada.

- Você reutilizará os endereços IP, as máscaras de rede e os gateways das plataformas originais nas novas plataformas.
- Os nomes de exemplo a seguir são usados neste procedimento, tanto em exemplos quanto em gráficos:
  - Local_A
    - Antes da atualização:
      - node_A_1-A700
      - node_A_2-A700
    - Após a atualização:
      - node_A_1-A900
      - node_A_2-A900
  - Local_B
    - Antes da atualização:
      - node_B_1-A700
      - node_B_2-A700
    - Após a atualização:
      - node_B_1-A900
      - node_B_2-A900

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

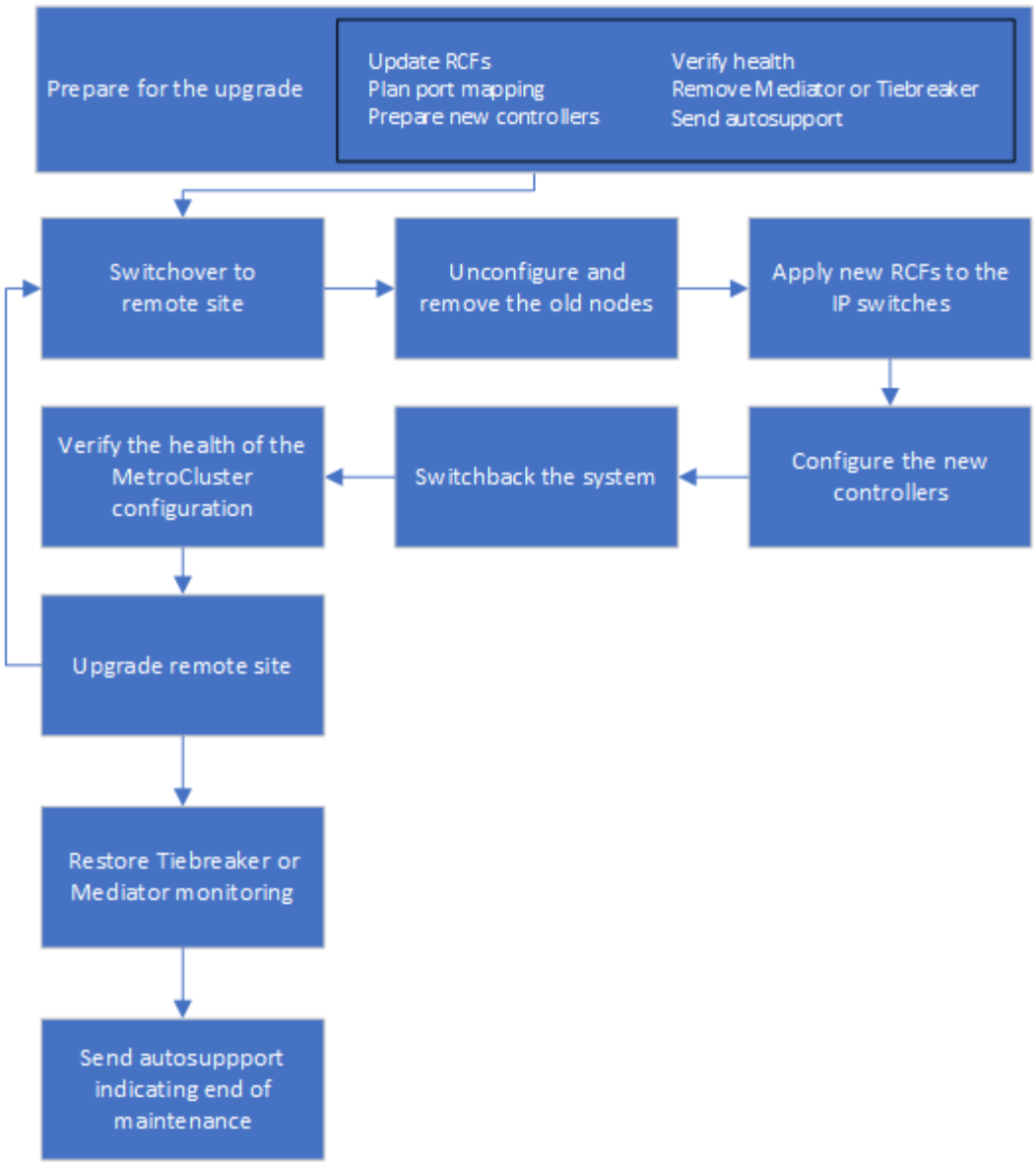
- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Fluxo de trabalho para atualizar controladores em uma configuração IP MetroCluster

Você pode usar o diagrama de fluxo de trabalho para ajudá-lo a Planejar as tarefas de atualização.



Prepare-se para a atualização

Antes de fazer quaisquer alterações na configuração do MetroCluster existente, você deve verificar a integridade da configuração, preparar as novas plataformas e executar outras tarefas diversas.

Limpe o slot 7 no controlador AFF A700 ou FAS9000

A configuração do MetroCluster em um AFF A900 ou FAS9500 usa uma de cada uma das portas nas placas de DR localizadas nos slots 5 e 7. Antes de iniciar a atualização, se houver placas no slot 7 no AFF A700 ou no FAS9000, você deve movê-las para outros slots para todos os nós do cluster.

Atualize os arquivos RCF do switch MetroCluster antes de atualizar os controladores

Você deve atualizar os arquivos RCF nos switches MetroCluster ao executar essa atualização. A tabela a seguir fornece os intervalos de VLAN suportados para configurações IP AFF A900/FAS9500 MetroCluster.

Modelo de plataforma	IDs de VLAN suportadas

• AFF A900 ou FAS9500	• 10 • 20 • Qualquer valor no intervalo de 101 a 4096 inclusive.

- Se o switch não estiver configurado com a versão de arquivo RCF mínima suportada, você deverá atualizar o arquivo RCF. Para obter a versão correta do arquivo RCF para o modelo do switch, consulte o "Ferramenta RcfFileGenerator". As etapas a seguir são para o aplicativo de arquivo RCF.

Passos

1. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch IP NVIDIA para os padrões de fábrica"

2. Baixe e instale os arquivos RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Baixe e instale os arquivos Broadcom RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

Mapear portas dos nós antigos para os novos nós

Ao fazer a atualização de um AFF A700 para um AFF A900 ou FAS9000 para FAS9500, você não altera as portas de rede de dados, as portas de adaptador SAN FCP e as portas de storage SAS e NVMe. Os LIFs de dados permanecem onde estão durante e após o upgrade. Portanto, não é necessário mapear as portas de rede dos nós antigos para os novos nós.

Verifique a integridade do MetroCluster antes da atualização do site

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a atualização.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:

   a. Verifique se os nós são multipathed: Mais
   `node run -node node-name sysconfig -a`

   Você deve emitir este comando para cada nó na configuração do MetroCluster.

   b. Verifique se não há discos quebrados na configuração
   `storage disk show -broken`

   Você deve emitir este comando em cada nó na configuração do MetroCluster.

c. Verifique se existem alertas de saúde:

```
system health alert show
```

Você deve emitir este comando em cada cluster.

d. Verifique as licenças nos clusters:

```
system license show
```

Você deve emitir este comando em cada cluster.

e. Verifique os dispositivos conetados aos nós:

```
network device-discovery show
```

Você deve emitir este comando em cada cluster.

f. Verifique se o fuso horário e a hora estão definidos corretamente em ambos os sites:

```
cluster date show
```

Você deve emitir este comando em cada cluster. Você pode usar o `cluster date` comando para configurar a hora e o fuso horário.

2. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
   a. Confirme a configuração do MetroCluster e se o modo operacional é `normal`
   `metrocluster show`
   b. Confirme que todos os nós esperados são mostrados
   `metrocluster node show`
   c. Emita o seguinte comando:

```
metrocluster check run
```

   d. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

3. Verifique o cabeamento do MetroCluster com a ferramenta Config Advisor.
   a. Baixe e execute o Config Advisor.

   "NetApp Downloads: Config Advisor"

   b. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Reúna informações antes da atualização

Antes de atualizar, você deve reunir informações para cada um dos nós e, se necessário, ajustar os domínios de broadcast de rede, remover quaisquer VLANs e grupos de interfaces e reunir informações de criptografia.

Passos

1. Registre o cabeamento físico de cada nó, rotulando os cabos conforme necessário para permitir o cabeamento correto dos novos nós.
2. Reúna a saída dos seguintes comandos para cada nó:
   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`
   - `vserver fcp initiator show`
   - `storage disk show`
   - `metrocluster configuration-settings interface show`
3. Reúna os UUIDs para o site_B (o site cujas plataformas estão sendo atualizadas): `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Esses valores devem ser configurados com precisão nos novos módulos do controlador site_B para garantir uma atualização bem-sucedida. Copie os valores para um arquivo para que você possa copiá-los para os comandos apropriados posteriormente no processo de atualização. O exemplo a seguir mostra a saída do comando com os UUIDs:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
   (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

É recomendável que você grave os UUIDs em uma tabela semelhante à seguinte.

Cluster ou nó	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1-A700	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2-A700	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1-A700	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2-A700	a9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Se os nós de MetroCluster estiverem em uma configuração de SAN, colete as informações relevantes.

   Você deve reunir a saída dos seguintes comandos:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Se o volume raiz estiver criptografado, colete e salve a senha usada para o gerenciador de chaves: `security key-manager backup show`
6. Se os nós do MetroCluster estiverem usando criptografia para volumes ou agregados, copie informações

sobre as chaves e senhas. Para obter informações adicionais, "Fazer backup manual de informações de gerenciamento de chaves integradas"consulte .

a. Se o Gerenciador de chaves integrado estiver configurado: `security key-manager onboard show-backup`Você precisará da senha mais tarde no procedimento de atualização.

b. Se o gerenciamento de chaves empresariais (KMIP) estiver configurado, emita os seguintes comandos:

```
security key-manager external show -instance
security key-manager key query
```

7. Reúna as IDs do sistema dos nós existentes:
`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

A saída a seguir mostra as unidades reatribuídas.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- ------------------
------------------ ---------------------
1           cluster_A node_A_1-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322           537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323           537403324
1           cluster_B node_B_2-A700   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Remova a monitorização do Mediator ou do tiebreaker

Antes de atualizar as plataformas, você deve remover o monitoramento se a configuração do MetroCluster for monitorada com o utilitário tiebreaker ou Mediator.

Passos

1. Colete a saída para o seguinte comando:

```
storage iscsi-initiator show
```

2. Remova a configuração do MetroCluster existente do tiebreaker, Mediator ou outro software que possa iniciar o switchover.

Se você estiver usando…	Use este procedimento…
Desempate	"Remoção das configurações do MetroCluster" No *MetroCluster Tiebreaker Instalação e Configuração conteúdo*
Mediador	Execute o seguinte comando no prompt do ONTAP: `metrocluster configuration-settings mediator remove`
Aplicativos de terceiros	Consulte a documentação do produto.

Envie uma mensagem AutoSupport personalizada antes da manutenção

Antes de realizar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Inicie sessão no cluster.
2. Chame uma mensagem AutoSupport indicando o início da manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   O `maintenance-window-in-hours` parâmetro especifica o comprimento da janela de manutenção, com um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repita estas etapas no site do parceiro.

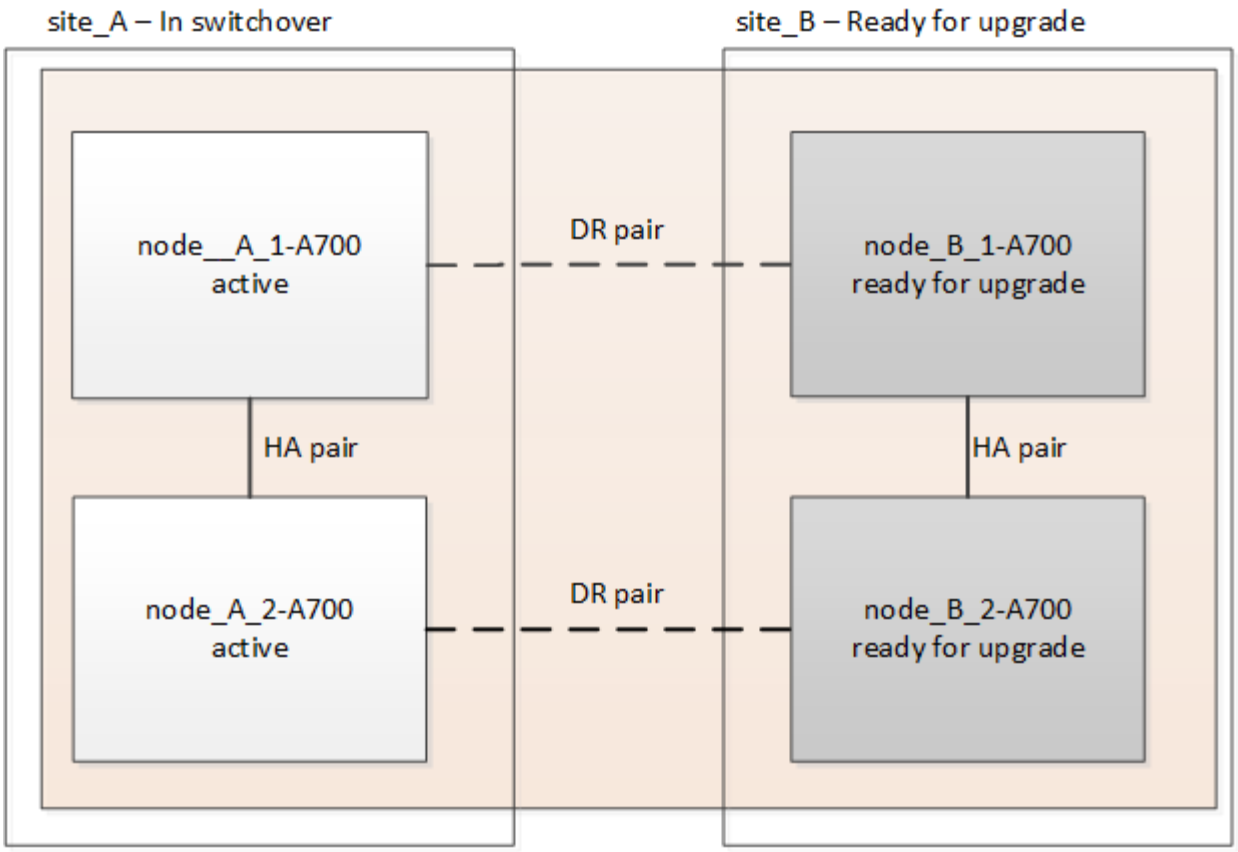
Alterne a configuração do MetroCluster

Você deve alternar a configuração para site_A para que as plataformas no site_B possam ser atualizadas.

Sobre esta tarefa

Esta tarefa tem de ser executada no site_A.

Depois de concluir esta tarefa, site_A está ativo e fornecendo dados para ambos os sites. Site_B está inativo e pronto para iniciar o processo de atualização.



Passos

1. Alterne a configuração do MetroCluster para site_A para que os nós do site_B possam ser atualizados:

   a. Execute o seguinte comando no site_A:

      `metrocluster switchover -controller-replacement true`

      A operação pode levar vários minutos para ser concluída.

   b. Monitorize a operação de comutação:

      `metrocluster operation show`

   c. Após a conclusão da operação, confirme se os nós estão no estado de comutação:

      `metrocluster show`

   d. Verifique o status dos nós MetroCluster:

      `metrocluster node show`

   A recuperação automática de agregados após o switchover negociado é desativada durante a atualização do controlador. Os nós no site_B são interrompidos e parados no `LOADER` prompt.

Remova o módulo do controlador da plataforma AFF A700 ou FAS9000 e o NVS

Sobre esta tarefa

Se você ainda não está aterrado, aterre-se adequadamente.

Passos

1. Reúna os valores de bootarg de ambos os nós no site_B: `printenv`
2. Desligue o chassis no local_B.

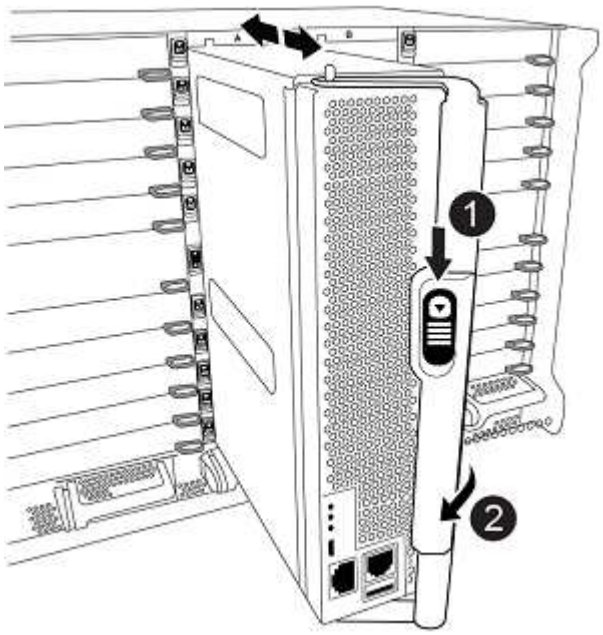
Retire o módulo do controlador AFF A700 ou FAS9000

Use o procedimento a seguir para remover o módulo do controlador AFF A700 ou FAS9000

Passos

1. Retire o cabo da consola, se existir, e o cabo de gestão do módulo do controlador antes de remover o módulo do controlador.
2. Desbloqueie e retire o módulo do controlador do chassis.

   a. Deslize o botão laranja na pega do came para baixo até que este se destranque.



	Botão de libertação do manípulo do excêntrico
	Pega do came

   a. Rode o manípulo do excêntrico de forma a desengatar completamente o módulo do controlador do chassis e, em seguida, deslize o módulo do controlador para fora do chassis. Certifique-se de que suporta a parte inferior do módulo do controlador enquanto o desliza para fora do chassis.

Retire o módulo de ruído, vibração e aspereza (NVS) do AFF A700 ou FAS9000

Use o procedimento a seguir para remover o módulo de ruído, vibração e aspereza (NVS) do AFF A700 ou do FAS9000.

Nota: O módulo NVS está no slot 6 e é o dobro da altura em comparação com outros módulos do sistema.

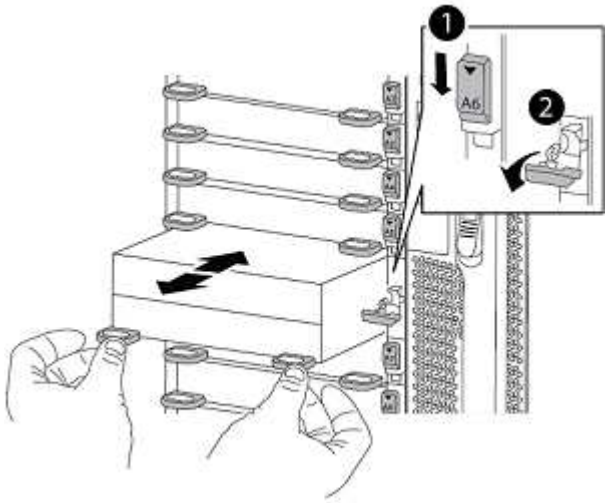
Passos

1. Desbloqueie e retire o NVS da ranhura 6.

   a. Prima o botão 'cam' com letras e numerado. O botão do came afasta-se do chassis.

   b. Rode o trinco da árvore de cames para baixo até estar na posição horizontal. O NVS desengata-se do chassis e desloca-se a alguns centímetros.

   c. Retire o NVS do chassis puxando as patilhas de puxar nas laterais da face do módulo.



	Trinco do came de e/S com letras e numerado
	Trinco de e/S completamente desbloqueado

2. Se você estiver usando módulos adicionais usados como dispositivos de coredump no AFF A700 ou no FAS9000 NVS, não os transfira para o AFF A900 ou o FAS9500 NVS. Não transfira quaisquer peças do módulo do controlador AFF A700 ou FAS9000 e do NVS para o módulo AFF A900 ou FAS9500.

Instale o AFF A900 ou o FAS9500 NVS e os módulos do controlador

Você deve instalar o AFF A900 ou o FAS9500 NVS e o módulo da controladora que recebeu no kit de atualização em ambos os nós no local_B. Não mova o dispositivo de coredump do módulo NVS AFF A700 ou FAS9000 para o módulo NVS AFF A900 ou FAS9500.

Sobre esta tarefa

Se você ainda não está aterrado, aterre-se adequadamente.

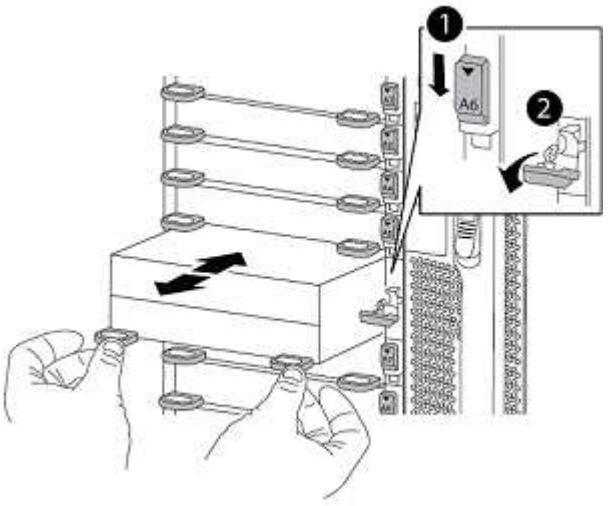
Instale o AFF A900 ou o FAS9500 NVS

Use o procedimento a seguir para instalar o AFF A900 ou o FAS9500 NVS no slot 6 de ambos os nós no local_B.

Passos

1. Alinhe o NVS com as bordas da abertura do chassi no slot 6.
2. Deslize suavemente o NVS para dentro da ranhura até que o trinco do came de e/S com letras e numerado comece a engatar com o pino do came de e/S e, em seguida, empurre o trinco do came de e/S

totalmente para cima para bloquear o NVS no devido lugar.



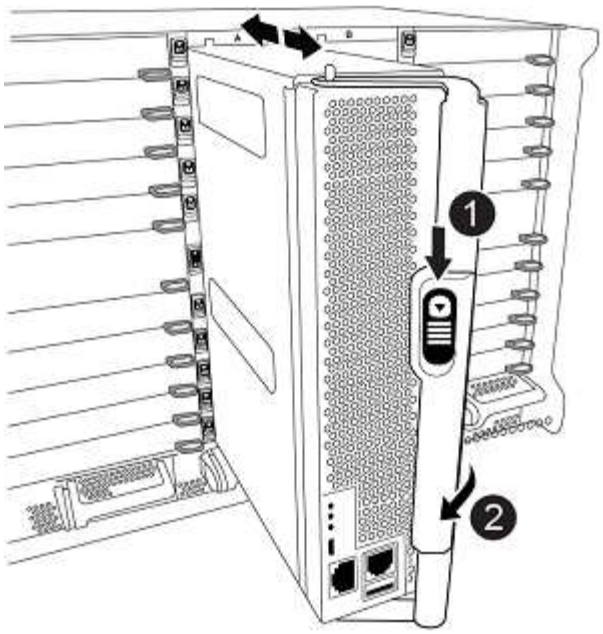
	Trinco do came de e/S com letras e numerado
	Trinco de e/S completamente desbloqueado

Instale o módulo do controlador AFF A900 ou FAS9500.

Use o procedimento a seguir para instalar o módulo do controlador AFF A900 ou FAS9500.

Passos

1. Alinhe a extremidade do módulo do controlador com a abertura no chassis e, em seguida, empurre cuidadosamente o módulo do controlador até meio do sistema.
2. Empurre firmemente o módulo do controlador para dentro do chassi até que ele atenda ao plano médio e esteja totalmente assentado. O trinco de bloqueio sobe quando o módulo do controlador está totalmente assente. Atenção: Para evitar danificar os conetores, não use força excessiva ao deslizar o módulo do controlador para dentro do chassis.
3. Cable as portas de gerenciamento e console ao módulo do controlador.



	Botão de libertação do manípulo do excêntrico
	Pega do came

4. Instale a segunda placa X91146A no slot 7 de cada nó.
   a. Mova a conexão e5b para E7B.
   b. Mova a conexão E5A para e5b.

> O slot 7 em todos os nós do cluster deve estar vazio como mencionado na Mapear portas dos nós antigos para os novos nós seção.

5. LIGUE o chassi e conete-o ao console serial.
6. Após a inicialização do BIOS, se o nó iniciar autoboot, interrompa o AUTOBOOT pressionando Control-C.
7. Depois que o autoboot é interrompido, os nós param no prompt DO Loader. Se você não interromper a tempo e o node1 iniciar o boot, aguarde que o prompt pressione Ctrl-C para entrar no menu de inicialização. Depois que o nó parar no menu de inicialização, use a opção 8 para reinicializar o nó e interromper o autoboot durante a reinicialização.
8. No prompt Loader, defina as variáveis de ambiente padrão: Set-defaults
9. Salve as configurações de variáveis de ambiente padrão:
   `saveenv`

Nós netboot no site_B

Depois de trocar o módulo de controladora AFF A900 ou FAS9500 e o NVS, você precisa netboot dos nós AFF A900 ou FAS9500 e instalar a mesma versão do ONTAP e o nível de patch que está sendo executado no cluster. O termo netboot significa que você está inicializando a partir de uma imagem ONTAP armazenada em um servidor remoto. Ao se preparar para netboot, você deve adicionar uma cópia da imagem de inicialização do ONTAP 9 a um servidor da Web que o sistema possa acessar. Não é possível verificar a versão do ONTAP instalada no suporte de arranque de um módulo controlador AFF A900 ou FAS9500, a menos que esteja

instalado num chassis e LIGADO. A versão do ONTAP na Mídia de inicialização do AFF A900 ou do FAS9500 deve ser a mesma que a versão do ONTAP em execução no sistema AFF A700 ou FAS9000 que está sendo atualizada e as imagens de inicialização principal e de backup devem corresponder. Você pode configurar as imagens executando um netboot seguido do `wipeconfig` comando no menu de inicialização. Se o módulo do controlador foi usado anteriormente em outro cluster, o `wipeconfig` comando limpa qualquer configuração residual na Mídia de inicialização.

Antes de começar

- Verifique se você pode acessar um servidor HTTP com o sistema.
- Você precisa baixar os arquivos de sistema necessários para o seu sistema e a versão correta do ONTAP a partir do site de suporte da NetApp.

Sobre esta tarefa

Você deve netboot dos novos controladores, se a versão do ONTAP instalada não for a mesma que a versão instalada nos controladores originais. Depois de instalar cada novo controlador, inicialize o sistema a partir da imagem ONTAP 9 armazenada no servidor Web. Em seguida, pode transferir os ficheiros corretos para o dispositivo multimédia de arranque para as subsequentes inicializações do sistema.

Passos

1. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.
2. Baixe o software ONTAP apropriado na seção de download de software do site de suporte da NetApp e armazene o `ontap-version_image.tgz` arquivo em um diretório acessível pela Web.
3. Mude para o diretório acessível pela Web e verifique se os arquivos necessários estão disponíveis.
4. A lista de diretórios deve conter ONTAP_version>_image.tgz.
5. Configure a conexão netboot escolhendo uma das seguintes ações.

> Você deve usar a porta de gerenciamento e o IP como conexão netboot. Não use um IP de LIF de dados ou uma interrupção de dados pode ocorrer enquanto a atualização está sendo realizada.

Se o protocolo de configuração dinâmica do host (DCHP) for…	Então…
Em execução	Configure a conexão automaticamente usando o seguinte comando no prompt do ambiente de inicialização: `ifconfig e0M -auto`

Não está em execução	Configure manualmente a conexão usando o seguinte comando no prompt do ambiente de inicialização: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> -dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` É o endereço IP do sistema de armazenamento. `<netmask>` é a máscara de rede do sistema de armazenamento. `<gateway>` é o gateway para o sistema de armazenamento. `<dns_addr>` É o endereço IP de um servidor de nomes na rede. Este parâmetro é opcional. `<dns_domain>` É o nome de domínio do serviço de nomes de domínio (DNS). Este parâmetro é opcional. NOTA: Outros parâmetros podem ser necessários para a sua interface. Insira `help ifconfig` no prompt do firmware para obter detalhes.

6. Execute netboot em node_B_1:
`netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   O `<path_to_the_web-accessible_directory>` deve levar ao local onde você baixou o `<ontap_version>\_image.tgz` em Passo 2.

   Não interrompa a inicialização.

7. Aguarde até que o node_B_1 esteja sendo executado no módulo controlador AFF A900 ou FAS9500 para inicializar e exibir as opções do menu de inicialização, conforme mostrado abaixo:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. No menu de inicialização, selecione a `(7) Install new software first.` opção esta opção de menu baixa e instala a nova imagem ONTAP no dispositivo de inicialização. OBSERVAÇÃO: Ignore a seguinte mensagem: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair.` Esta observação se aplica a atualizações de software ONTAP sem interrupções e não atualizações de controladora.

   Sempre use netboot para atualizar o novo nó para a imagem desejada. Se você usar outro método para instalar a imagem no novo controlador, a imagem incorreta pode ser instalada. Este problema aplica-se a todas as versões do ONTAP.

9. Se você for solicitado a continuar o procedimento, digite `y` e, quando solicitado, digite o URL: `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>\_image.tgz`
10. Conclua as seguintes subetapas para reinicializar o módulo do controlador:
    a. Introduza `n` para ignorar a recuperação da cópia de segurança quando vir o seguinte aviso: `Do you want to restore the backup configuration now? {y|n}`
    b. Entre `y to reboot when you see the following prompt: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}` no módulo do controlador reinicializa, mas pára no menu de inicialização porque o dispositivo de inicialização foi reformatado e os dados de configuração precisam ser restaurados.
11. No prompt, execute o `wipeconfig` comando para limpar qualquer configuração anterior na Mídia de inicialização:
    a. Quando vir a seguinte mensagem, responda `yes`: `This will delete critical system configuration, including cluster membership.` `Warning: do not run this option on a HA node that has been taken over.` `Are you sure you want to continue?:`
    b. O nó reinicializa para terminar o `wipeconfig` e, em seguida, pára no menu de inicialização.
12. Selecione a opção `5` para ir para o modo de manutenção a partir do menu de arranque. Responda `yes` aos prompts até que o nó pare no modo de manutenção e o prompt de comando '*>.
13. Repita estas etapas para netboot node_B_2.

Restaure a configuração do HBA

Dependendo da presença e configuração das placas HBA no módulo controlador, você precisa configurá-las corretamente para uso do seu site.

Passos

1. No modo de manutenção, configure as definições para quaisquer HBAs no sistema:
   a. Verifique as definições atuais das portas:

      `ucadmin show`

   b. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado…	Use este comando…

CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
Destino de FC	`fcadmin config -t target` *`adapter-name`*
Iniciador FC	`fcadmin config -t initiator` *`adapter-name`*

2. Sair do modo de manutenção:

   `halt`

   Depois de executar o comando, aguarde até que o nó pare no prompt DO Loader.

3. Inicialize o nó novamente no modo Manutenção para permitir que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

4. Verifique as alterações feitas:

Se você tem este tipo de HBA…	Use este comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Defina o estado de HA nos novos controladores e chassi

É necessário verificar o estado de HA dos controladores e do chassi e, se necessário, atualizar o estado para corresponder à configuração do sistema.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado HA para todos os componentes deve ser `mccip`.

2. Se o estado do sistema apresentado do controlador ou do chassis não estiver correto, defina o estado HA:

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

3. Parar o nó: `halt`

O nó deve parar no `LOADER>` prompt.

4. Em cada nó, verifique a data, a hora e o fuso horário do sistema: `show date`
5. Se necessário, defina a data em UTC ou GMT: `set date <mm/dd/yyyy>`
6. Verifique a hora usando o seguinte comando no prompt do ambiente de inicialização: `show time`
7. Se necessário, defina a hora em UTC ou GMT: `set time <hh:mm:ss>`
8. Guarde as definições: `saveenv`
9. Reunir variáveis de ambiente: `printenv`

Atualize os arquivos RCF do switch para acomodar as novas plataformas

Você deve atualizar os switches para uma configuração que suporte os novos modelos de plataforma.

Sobre esta tarefa

Você executa essa tarefa no site que contém os controladores que estão sendo atualizados no momento. Nos exemplos mostrados neste procedimento, estamos atualizando site_B primeiro.

Os switches no site_A serão atualizados quando os controladores no site_A forem atualizados.

Passos

1. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"
2. Baixe e instale os arquivos RCF.

   Siga as etapas na seção para o fornecedor do switch:

   - "Baixe e instale os arquivos Broadcom RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

Configure os novos controladores

Novos controladores devem estar prontos e cabeados neste momento.

Defina as variáveis MetroCluster IP bootarg

Certos valores de inicialização IP do MetroCluster devem ser configurados nos novos módulos do controlador. Os valores devem corresponder aos configurados nos módulos do controlador antigos.

Sobre esta tarefa

Nesta tarefa, você usará os UUIDs e IDs do sistema identificados anteriormente no procedimento de atualização no Reúna informações antes da atualização.

Passos

1. `LOADER>`No prompt, defina os seguintes bootargs nos novos nós no site_B:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   O exemplo a seguir define os valores para node_B_1-A900 usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   O exemplo a seguir define os valores para node_B_2-A900 usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. No prompt dos novos nós `LOADER`, defina os UUIDs:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Defina os UUIDs em node_B_1-A900.

      O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_1-A900:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Defina os UUIDs em node_B_2-A900:

O exemplo a seguir mostra os comandos para definir os UUIDs em node_B_2-A900:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Se os sistemas originais foram configurados para ADP, em cada prompt DO Loader dos nós de substituição, ative o ADP:

```
setenv bootarg.mcc.adp_enabled true
```

4. Defina as seguintes variáveis:

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> A `setenv bootarg.mcc.local_config_id` variável deve ser definida para o sys-id do módulo controlador **original**, node_B_1-A700.

a. Defina as variáveis em node_B_1-A900.

O exemplo a seguir mostra os comandos para definir os valores em node_B_1-A900:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Defina as variáveis em node_B_2-A900.

O exemplo a seguir mostra os comandos para definir os valores em node_B_2-A900:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Se estiver usando criptografia com gerenciador de chaves externo, defina os bootargs necessários:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Reatribuir discos agregados de raiz

Reatribua os discos agregados de raiz ao novo módulo de controladora, usando os sysids reunidos anteriormente.

Sobre esta tarefa

Estes passos são executados no modo de manutenção.

Passos

1. Inicialize o sistema no modo de manutenção:

   ```
   boot_ontap maint
   ```

2. Exiba os discos no node_B_1-A900 no prompt do modo de manutenção:

   ```
   disk show -a
   ```

   A saída do comando mostra a ID do sistema do novo módulo do controlador (1574774970). No entanto, os discos agregados de raiz ainda são propriedade do ID do sistema antigo (537403322). Este exemplo não mostra unidades de propriedade de outros nós na configuração do MetroCluster.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------              -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. Reatribua os discos agregados de raiz nos compartimentos de unidades às novas controladoras.

Se você estiver usando ADP…	Em seguida, use este comando…
Sim	`disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid`
Não	`disk reassign -s old-sysid -d new-sysid`

4. Reatribua os discos agregados de raiz nos compartimentos de unidades às novas controladoras:

   `disk reassign -s old-sysid -d new-sysid`

   O exemplo a seguir mostra a reatribuição de unidades em uma configuração não ADP:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verifique se os discos do agregado raiz estão corretamente reatribuídos à remoção antiga:

   ```
   disk show

   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                    DR HOME
------------             -------------            -----  -------------
-------------           -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Inicialize os novos controladores

Você deve inicializar os novos controladores, tomando cuidado para garantir que as variáveis bootarg estão corretas e, se necessário, executar as etapas de recuperação de criptografia.

Passos

1. Parar os novos nós:

   ```
   halt
   ```

2. Se o gerenciador de chaves externo estiver configurado, defina os bootargs relacionados:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Verifique se o parceiro-sysid é o atual:

   ```
   printenv partner-sysid
   ```

   Se o parceiro-sysid não estiver correto, defina-o:

   ```
   setenv partner-sysid partner-sysID
   ```

4. Exiba o menu de inicialização do ONTAP:

   ```
   boot_ontap menu
   ```

5. Se a criptografia raiz for usada, selecione a opção do menu de inicialização para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção 10 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves
Gerenciamento de chaves externas	Opção 11 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves

6. No menu de inicialização, `(6) Update flash from backup config` selecione .

   A opção 6 reiniciará o nó duas vezes antes de concluir.

   Responda `y` aos prompts de alteração de ID do sistema. Aguarde a segunda mensagem de reinicialização:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Interrompa o AUTOBOOT para parar os controladores NO Loader.

   Em cada nó, verifique os bootargs definidos "Configurando as variáveis de inicialização IP do MetroCluster"e corrija quaisquer valores incorretos. Apenas passe para a próxima etapa depois de verificar os valores de bootarg.

8. Verifique se o parceiro-sysid está correto:

   ```
   printenv partner-sysid
   ```

   Se o parceiro-sysid não estiver correto, defina-o:

`setenv partner-sysid partner-sysID`

9. Se a criptografia raiz for usada, selecione a opção do menu de inicialização para a configuração de gerenciamento de chaves.

Se você estiver usando…	Selecione esta opção do menu de arranque…
Gerenciamento de chaves integrado	Opção 10 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves
Gerenciamento de chaves externas	Opção 11 e siga as instruções para fornecer as entradas necessárias para recuperar ou restaurar a configuração do gerenciador de chaves

Você precisa executar o procedimento de recuperação selecionando a opção 10 ou a opção 11, dependendo da configuração do gerenciador de chaves e a opção 6 no prompt do menu de inicialização. Para inicializar completamente os nós, talvez seja necessário executar o procedimento de recuperação continuado pela opção 1 (inicialização normal).

10. Aguarde que os novos nós, node_B_1-A900 e node_B_2-A900 iniciem.

Se um dos nós estiver no modo de aquisição, execute um giveback usando o `storage failover giveback` comando.

11. Se a criptografia for usada, restaure as chaves usando o comando correto para sua configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gerenciamento de chaves integrado	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .
Gerenciamento de chaves externas	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Verifique se todas as portas estão em um domínio de broadcast:

a. Veja os domínios de broadcast:

`network port broadcast-domain show`

b. Adicione quaisquer portas a um domínio de broadcast conforme necessário.

"Adicionar ou remover portas de um domínio de broadcast"

c. Recrie VLANs e grupos de interface conforme necessário.

A associação de VLAN e grupo de interface pode ser diferente da do nó antigo.

"Criando um VLAN"

"Combinando portas físicas para criar grupos de interface"

Verifique e restaure a configuração do LIF

Verifique se os LIFs estão hospedados em nós e portas apropriados, conforme mapeados no início do procedimento de atualização.

Sobre esta tarefa

- Esta tarefa é executada no site_B.
- Consulte o plano de mapeamento de portas que criou Mapear portas dos nós antigos para os novos nós

Passos

1. Verifique se os LIFs estão hospedados no nó e nas portas apropriadas antes do switchback.

   a. Mude para o nível de privilégio avançado:

      `set -privilege advanced`

   b. Substituir a configuração da porta para garantir o posicionamento correto do LIF:

      `vserver config override -command "network interface modify -vserver` *`vserver_name`* `-home-port` *`active_port_after_upgrade`* `-lif` *`lif_name`* `-home-node` *`new_node_name`*"

   Ao entrar no comando Network Interface Modify dentro `vserver config override` do comando, não é possível usar o recurso Tab Autocomplete. Você pode criar a rede `interface modify` usando o autocomplete e, em seguida, incorporá-la no `vserver config override` comando.

   a. Voltar ao nível de privilégio de administrador:

      `set -privilege admin`

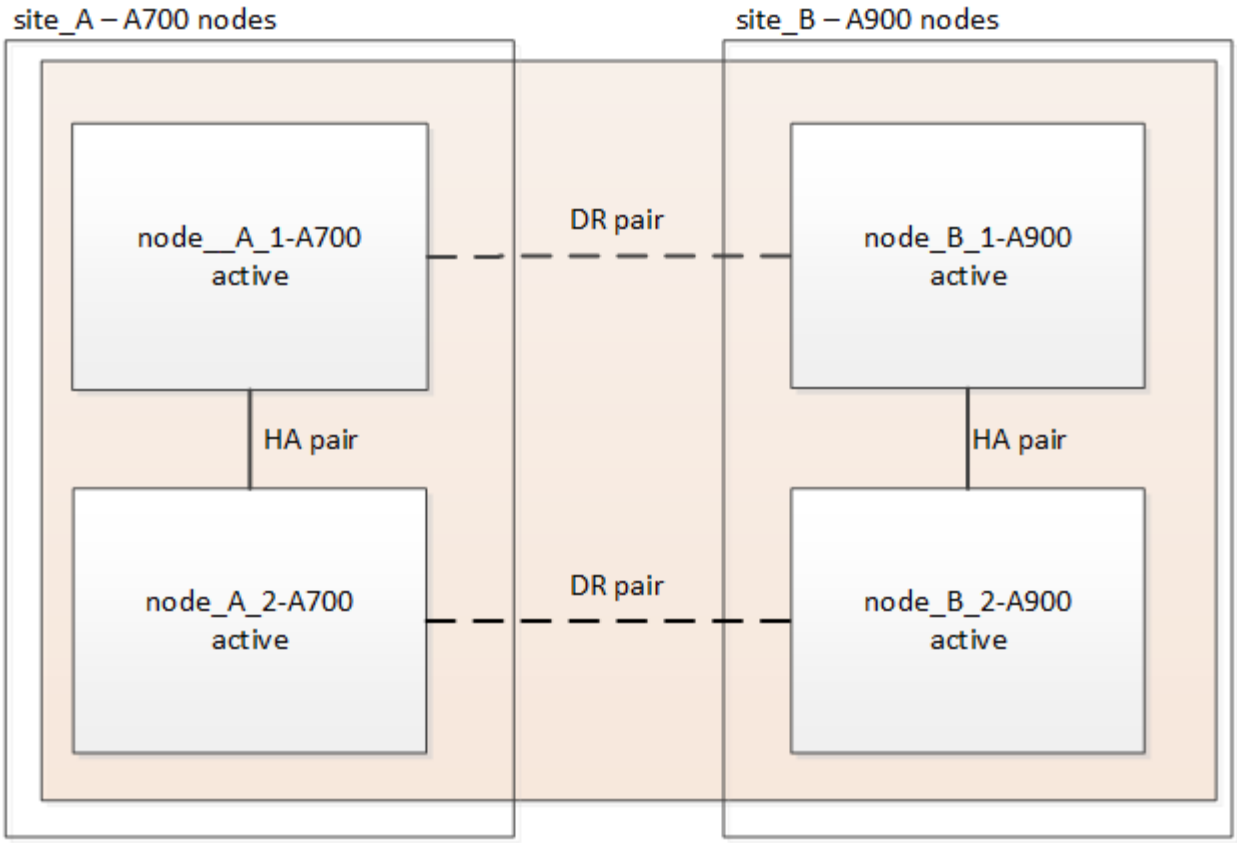
2. Reverter as interfaces para o seu nó inicial:

   `network interface revert * -vserver` *`vserver-name`*

   Execute esta etapa em todas as SVMs, conforme necessário.

Volte a ativar a configuração do MetroCluster

Nesta tarefa, você executará a operação de switchback e a configuração do MetroCluster retornará à operação normal. Os nós no site_A ainda estão aguardando atualização.



Passos

1. Emita o `metrocluster node show` comando de site_B e verifique a saída.
   a. Verifique se os novos nós estão representados corretamente.
   b. Verifique se os novos nós estão em "aguardando pelo estado de switchback".
2. Execute a recuperação e o switchback executando os comandos necessários de qualquer nó no cluster ativo (o cluster que não está sendo atualizado).
   a. Curar os agregados de dados
   `metrocluster heal aggregates`
   b. Curar os agregados de raiz:

   ```
   metrocluster heal root
   ```

   c. Comutar o cluster:

   ```
   metrocluster switchback
   ```

3. Verifique o progresso do funcionamento do interrutor de comutação:

   ```
   metrocluster show
   ```

   A operação de switchback ainda está em andamento quando a saída exibe `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

A operação de comutação está concluída quando a saída exibe normal:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o `metrocluster config-replication resync-status show` comando. Este comando está no nível de privilégio avançado.

Verifique a integridade da configuração do MetroCluster

Depois de atualizar os módulos do controlador, você deve verificar a integridade da configuração do MetroCluster.

Sobre esta tarefa

Esta tarefa pode ser executada em qualquer nó na configuração do MetroCluster.

Passos

1. Verifique o funcionamento da configuração do MetroCluster:
   a. Confirme a configuração do MetroCluster e se o modo operacional está normal
   `metrocluster show`
   b. Execute uma verificação MetroCluster
   `metrocluster check run`
   c. Apresentar os resultados da verificação MetroCluster:

   ```
   metrocluster check show
   ```

2. Verifique a conetividade e o status do MetroCluster.

a. Verifique as conexões IP do MetroCluster:

```
storage iscsi-initiator show
```

b. Verifique se os nós estão operando:

```
metrocluster node show
```

c. Verifique se as interfaces IP do MetroCluster estão ativas:

```
metrocluster configuration-settings interface show
```

d. Verifique se o failover local está ativado:

```
storage failover show
```

Atualize os nós no site_A

Você deve repetir as tarefas de atualização no site_A.

Passos

1. Repita as etapas para atualizar os nós no site_A, começando com Prepare-se para a atualização.

   À medida que você executa as tarefas, todas as referências de exemplo aos sites e nós são invertidas. Por exemplo, quando o exemplo é dado para o switchover de site_A, você irá mudar de site_B.

Restaure o monitoramento do tiebreaker ou do Mediator

Depois de concluir a atualização da configuração do MetroCluster, você pode retomar o monitoramento com o utilitário tiebreaker ou Mediator.

Passos

1. Restaure o monitoramento, se necessário, usando o procedimento para sua configuração.

Se você estiver usando…	Use este procedimento
Desempate	"Adição de configurações do MetroCluster" Na seção *MetroCluster tiebreaker Installation and Configuration*.
Mediador	"Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster" Na seção *Instalação e Configuração IP do MetroCluster*.
Aplicativos de terceiros	Consulte a documentação do produto.

Envie uma mensagem AutoSupport personalizada após a manutenção

Depois de concluir a atualização, você deve enviar uma mensagem AutoSupport indicando o fim da

manutenção, para que a criação automática de casos possa ser retomada.

Passos

1. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.

   a. Execute o seguinte comando
   `system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repita o comando no cluster de parceiros.

Atualizando uma configuração de MetroCluster FC de quatro nós

Você pode atualizar os controladores e o storage em uma configuração de MetroCluster de quatro nós, expandindo a configuração para se tornar uma configuração de oito nós e removendo o grupo de recuperação de desastres (DR) antigo.

Sobre esta tarefa

Referências a "nós antigos" significam os nós que você pretende substituir.

- Somente é possível atualizar modelos de plataforma específicos usando esse procedimento em uma configuração MetroCluster FC.
  - Para obter informações sobre quais combinações de atualização de plataforma são suportadas, consulte a tabela de atualização do MetroCluster FC "Escolher um método de atualização do sistema"no .

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

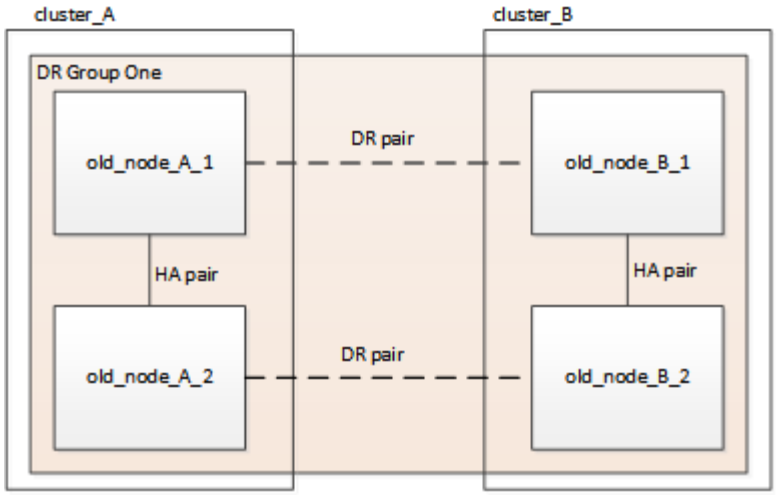
Execute o procedimento de atualização

Siga as etapas a seguir para atualizar a configuração do MetroCluster FC.

Passos

1. Reúna informações dos nós antigos.

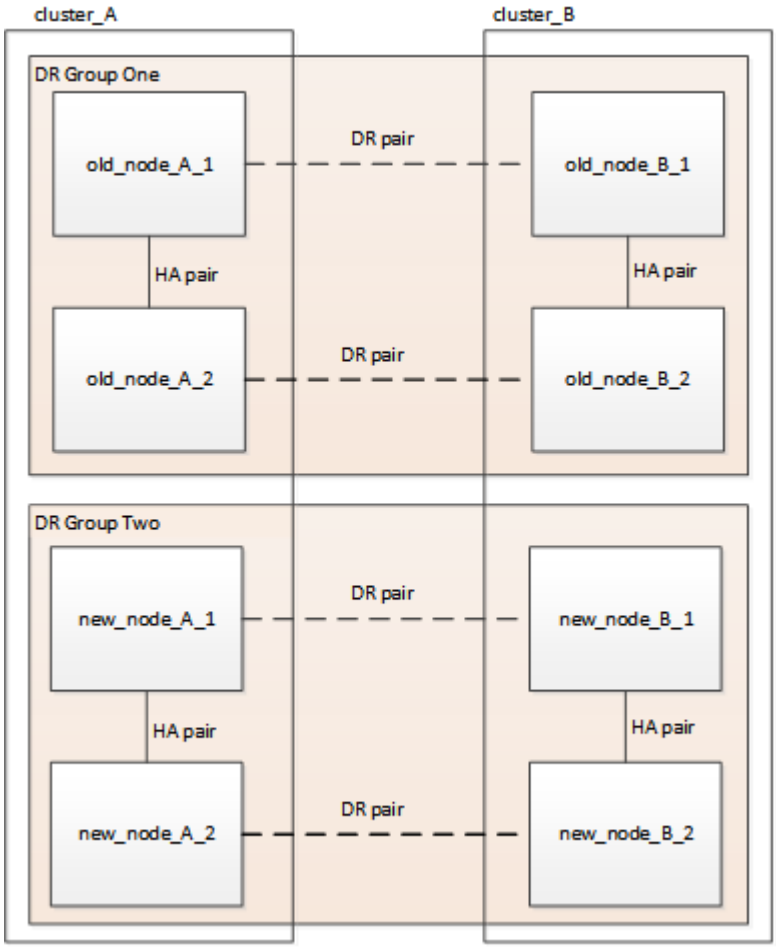
   Nesta fase, a configuração de quatro nós aparece como mostrado na seguinte imagem:



2. Execute todas as etapas do procedimento de expansão de quatro nós para o tipo MetroCluster.

   "Expansão de uma configuração de FC MetroCluster de quatro nós para uma configuração de oito nós"

   Quando o procedimento de expansão estiver concluído, a configuração aparece como mostrado na imagem a seguir:



3. Mova os volumes CRS.

   Execute as etapas em "Mover um volume de metadados nas configurações do MetroCluster".

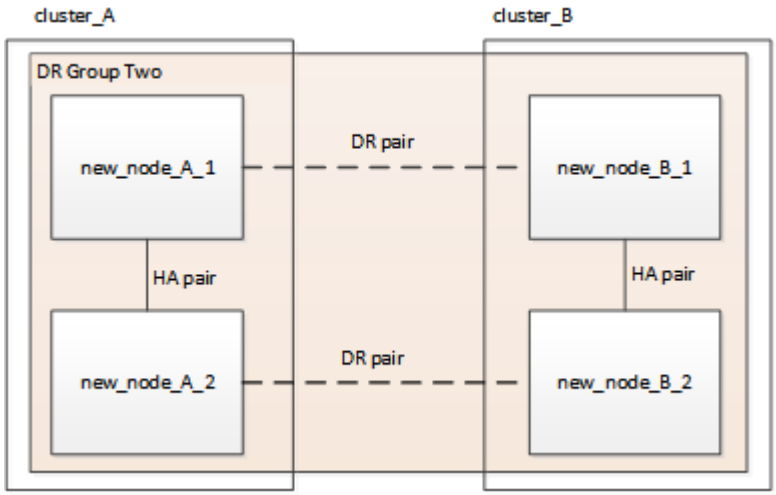
4. Mova os dados dos nós antigos para novos nós usando os seguintes procedimentos:
   a. Execute todas as etapas em "Crie um agregado e mova volumes para os novos nós".

      Você pode optar por espelhar o agregado quando ou depois que ele é criado.

   b. Execute todas as etapas em "Mova LIFs de dados que não são SAN e LIFs de gerenciamento de cluster para os novos nós".
   c. Execute todas as etapas em "Excluir SAN LIFs não é mais necessário dos nós originais".
5. Siga as etapas do procedimento para remover o grupo de RD antigo.

   "Removendo um grupo de recuperação de desastres"

   Depois de remover o antigo grupo de DR (grupo de DR um), a configuração aparece como mostrado na imagem a seguir:



Atualizar uma configuração IP MetroCluster de quatro ou oito nós (ONTAP 9.8 e posterior)

Você pode usar este procedimento para atualizar controladores e storage em configurações de quatro nós ou oito nós.

A partir do ONTAP 9.13,1, é possível atualizar os controladores e o armazenamento em uma configuração IP MetroCluster de oito nós expandindo a configuração para se tornar uma configuração temporária de doze nós e, em seguida, remover os grupos de recuperação de desastres (DR) antigos.

A partir do ONTAP 9.8, é possível atualizar os controladores e o armazenamento em uma configuração IP MetroCluster de quatro nós expandindo a configuração para se tornar uma configuração temporária de oito nós e, em seguida, remover o antigo grupo de DR.

Sobre esta tarefa

- Se você tiver uma configuração de oito nós, seu sistema deve estar executando o ONTAP 9.13,1 ou posterior.
- Se você tiver uma configuração de quatro nós, seu sistema deve estar executando o ONTAP 9.8 ou posterior.

- Se você também estiver atualizando os switches IP, deverá atualizá-los antes de executar este procedimento de atualização.
- Este procedimento descreve as etapas necessárias para atualizar um grupo de RD de quatro nós. Se você tiver uma configuração de oito nós (dois grupos de DR), poderá atualizar um ou ambos os grupos de DR.

  Se você atualizar ambos os grupos de DR, precisará atualizar um grupo de DR de cada vez.
- Referências a "nós antigos" significam os nós que você pretende substituir.
- Para configurações de oito nós, a combinação de plataforma MetroCluster de oito nós de origem e destino precisa ser compatível.

  Se você atualizar ambos os grupos de DR, a combinação de plataforma pode não ser suportada depois de atualizar o primeiro grupo de DR. É necessário atualizar os dois grupos de DR para obter uma configuração de oito nós compatível.
- Você só pode atualizar modelos de plataforma específicos usando este procedimento em uma configuração IP do MetroCluster.
  - Para obter informações sobre quais combinações de atualização de plataforma são suportadas, consulte a tabela de atualização de IP do MetroCluster no "Escolher um método de atualização do sistema".
- Aplicam-se os limites inferiores das plataformas de origem e destino. Se você fizer a transição para uma plataforma superior, os limites da nova plataforma serão aplicados somente após a conclusão da atualização técnica de todos os grupos de DR.
- Se você executar uma atualização técnica para uma plataforma com limites inferiores à plataforma de origem, você deve ajustar e reduzir os limites para estar em, ou abaixo, os limites da plataforma de destino antes de executar este procedimento.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".
- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Execute o procedimento de atualização

Siga as etapas a seguir para atualizar a configuração IP do MetroCluster.

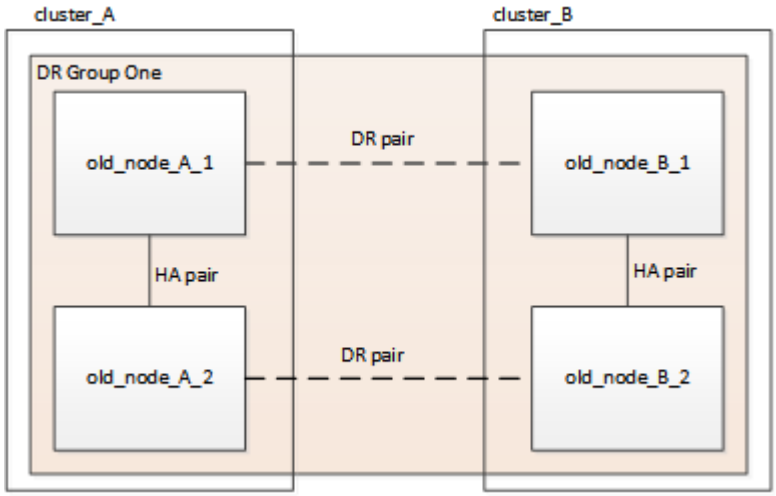
Passos

1. Verifique se você tem um domínio de broadcast padrão criado nos nós antigos.

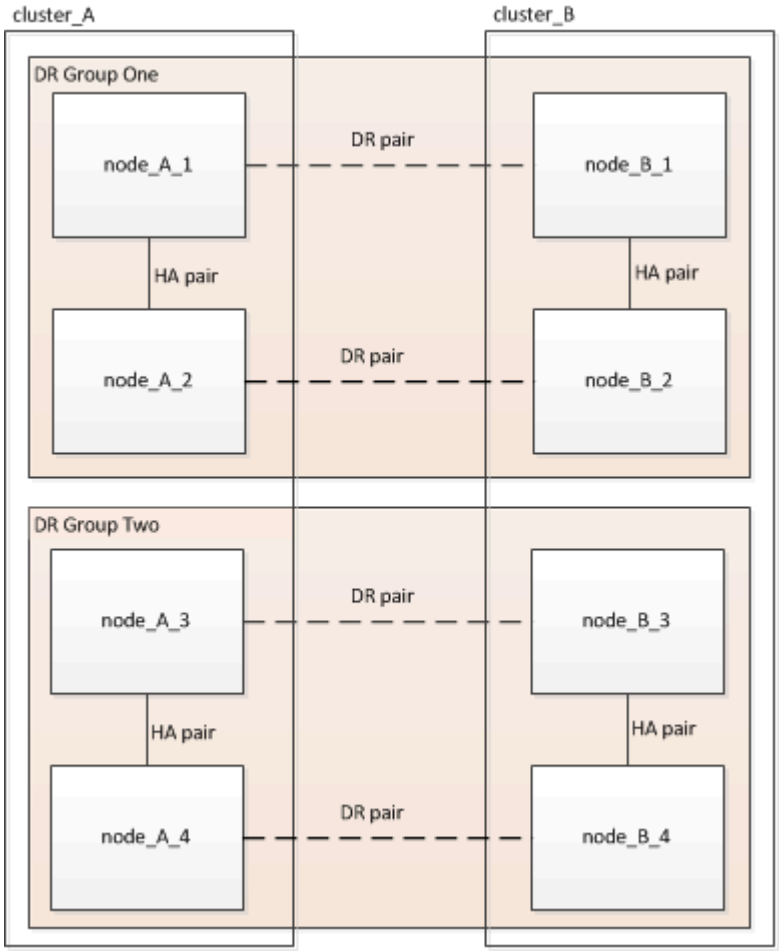
Quando você adiciona novos nós a um cluster existente sem um domínio de broadcast padrão, as LIFs de gerenciamento de nós são criadas para os novos nós usando identificadores únicos universais (UUIDs) em vez dos nomes esperados. Para obter mais informações, consulte o artigo da base de dados de Conhecimento "LIFs de gerenciamento de nós em nós recém-adicionados gerados com nomes UUID" .

2. Reúna informações dos nós antigos.

   Nesta fase, a configuração de quatro nós aparece como mostrado na seguinte imagem:



   A configuração de oito nós aparece como mostrado na imagem a seguir:



3. Para impedir a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a atualização está em andamento.

   a. Execute o seguinte comando
   `system node autosupport invoke -node * -type all -message "MAINT=10h Upgrading old-model to new-model"`

   O exemplo a seguir especifica uma janela de manutenção de 10 horas. Você pode querer permitir tempo adicional, dependendo do seu plano.

   Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Repita o comando no cluster de parceiros.

4. Se a criptografia de ponta a ponta estiver ativada, siga as etapas para "Desative a criptografia de ponta a ponta".

5. Remova a configuração do MetroCluster existente do tiebreaker, Mediator ou outro software que possa iniciar o switchover.

Se você estiver usando…	Use este procedimento…
Desempate	a. Use o comando tiebreaker CLI `monitor remove` para remover a configuração do MetroCluster. No exemplo a seguir, "'cluster_A" é removido do software: `NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.` b. Confirme se a configuração do MetroCluster foi removida corretamente usando o comando tiebreaker CLI `monitor show -status`. `NetApp MetroCluster Tiebreaker :> monitor show -status`

Mediador	Execute o seguinte comando no prompt do ONTAP: `metrocluster configuration-settings mediator remove`
Aplicativos de terceiros	Consulte a documentação do produto.

6. Execute todas as etapas em "Expandindo uma configuração IP do MetroCluster"para adicionar os novos nós e o storage à configuração.

   Quando o procedimento de expansão estiver concluído, a configuração temporária é apresentada conforme ilustrado nas seguintes imagens:

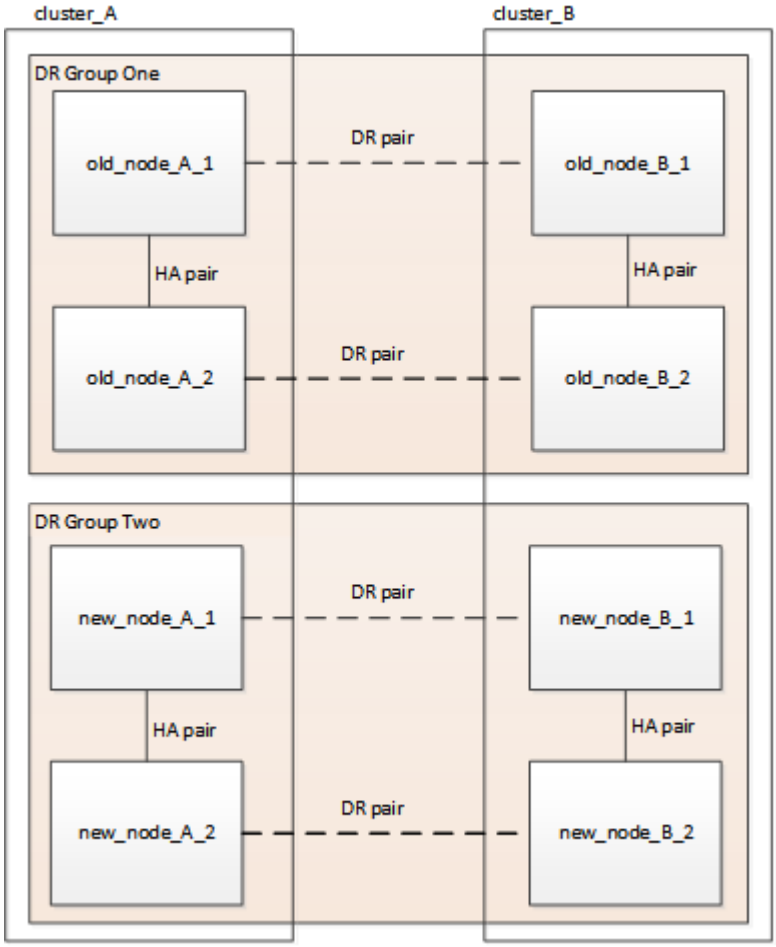


Figura 1. Configuração temporária de oito nós

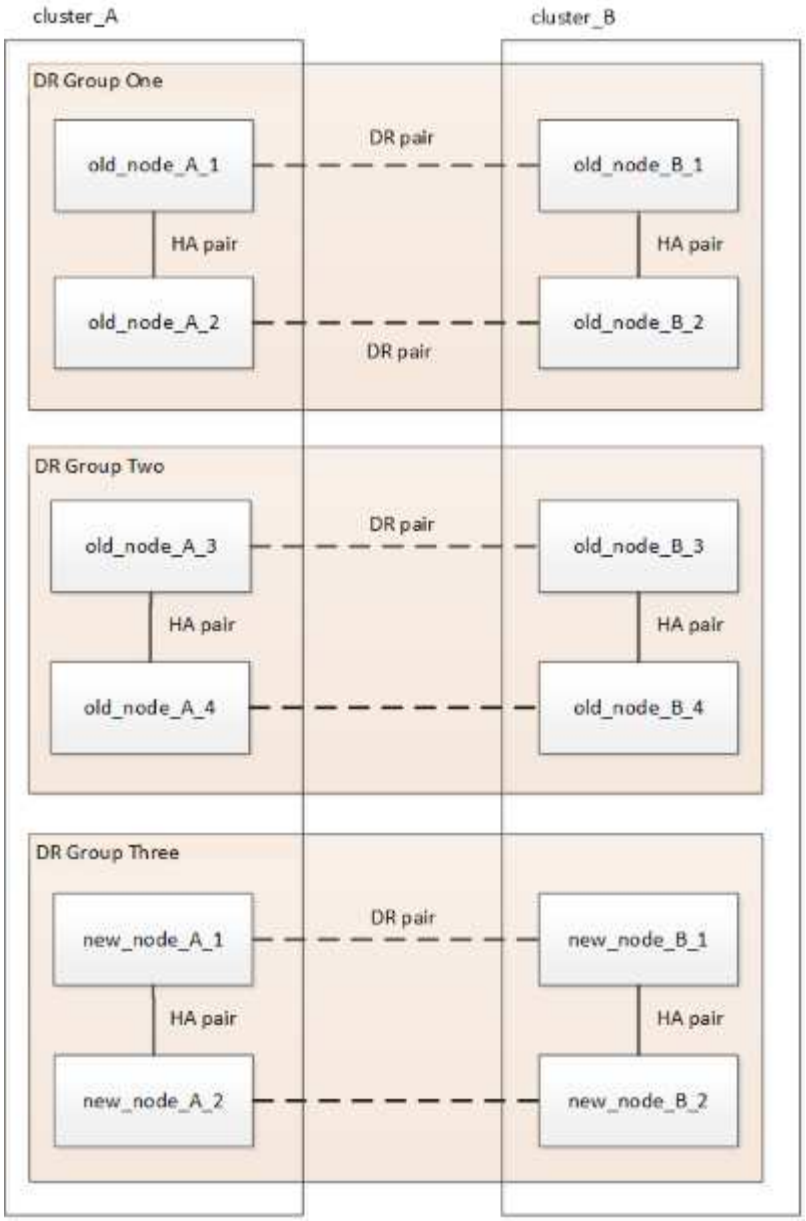


Figura 2. Configuração temporária de doze nós

7. Confirme se o takeover é possível e os nós estão conectados executando o seguinte comando em ambos os clusters:

   `storage failover show`

```
cluster_A::> storage failover show
                                    Takeover
Node           Partner              Possible    State Description
-------------- -------------------- ---------   ------------------
Node_FC_1      Node_FC_2              true      Connected to Node_FC_2
Node_FC_2      Node_FC_1              true      Connected to Node_FC_1
Node_IP_1      Node_IP_2              true      Connected to Node_IP_2
Node_IP_2      Node_IP_1              true      Connected to Node_IP_1
```

8. Mova os volumes CRS.

   Execute as etapas em "Movimentação de um volume de metadados nas configurações do MetroCluster".

9. Mova os dados dos nós antigos para os novos nós usando os seguintes procedimentos:
   a. Execute todas as etapas em "Crie um agregado e mova volumes para os novos nós".

      Você pode optar por espelhar o agregado quando ou depois que ele é criado.

   b. Execute todas as etapas em "Mova LIFs de dados que não são SAN e LIFs de gerenciamento de cluster para os novos nós".
10. Modifique o endereço IP para o ponto de cluster dos nós transicionados para cada cluster:
    a. Identifique o peer cluster_A usando o `cluster peer show` comando:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

       i. Modifique o endereço IP peer cluster_A:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

    b. Identifique o peer cluster_B usando o `cluster peer show` comando:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

       i. Modifique o endereço IP peer cluster_B:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

    c. Verifique se o endereço IP do peer do cluster está atualizado para cada cluster:

       i. Verifique se o endereço IP é atualizado para cada cluster usando o `cluster peer show -instance` comando.

          O `Remote Intercluster Addresses` campo nos exemplos a seguir exibe o endereço IP

atualizado.

Exemplo para cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_B
                     Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+
Exemplo para cluster_B

```
cluster_B::> cluster peer show -instance

                        Peer Cluster Name: cluster_A
            Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
             IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

11. Siga as etapas em "Removendo um grupo de recuperação de desastres" para remover o grupo de RD antigo.
12. Se você quiser atualizar ambos os grupos de DR em uma configuração de oito nós, repita todo o procedimento para cada grupo de DR.

    Depois de remover o antigo grupo DR, a configuração aparece como mostrado nas seguintes imagens:

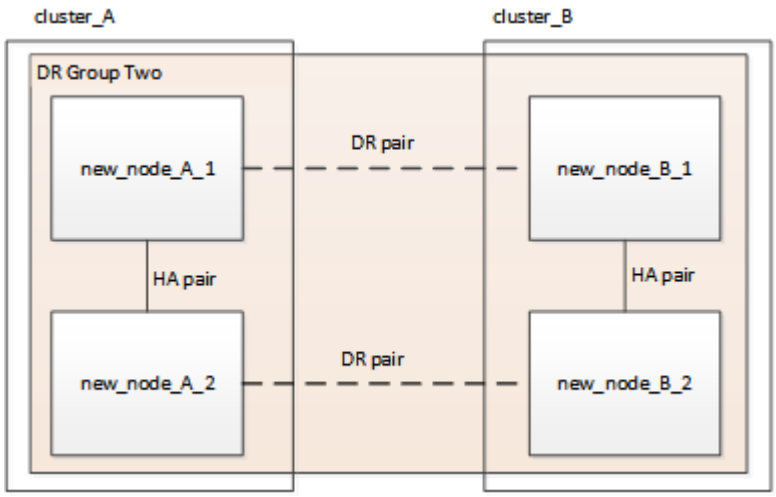


Figura 3. Configuração de quatro nós

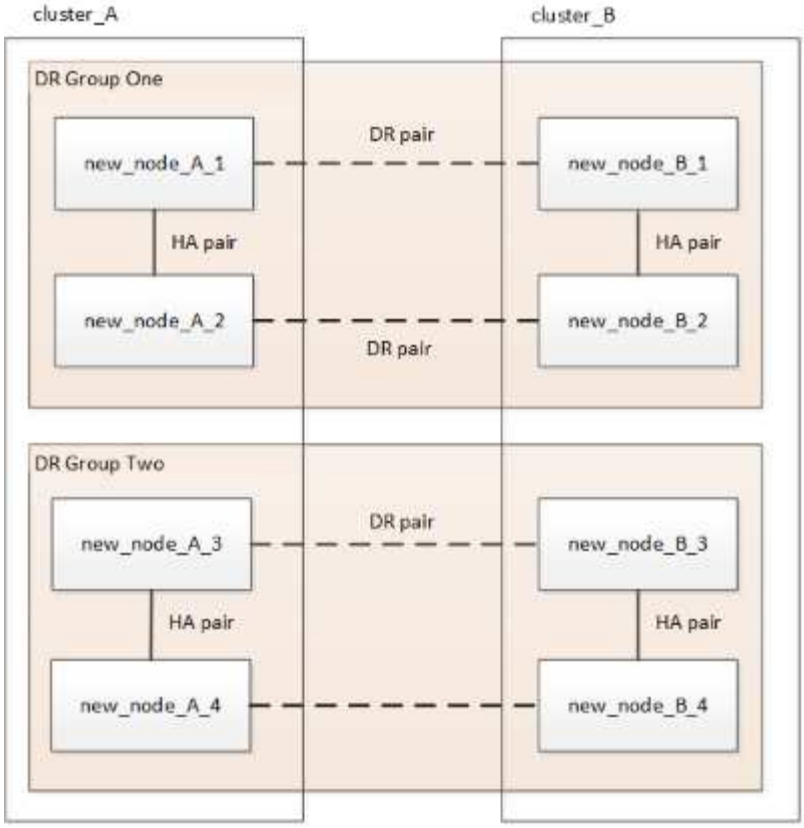


Figura 4. Configuração de oito nós

13. Confirme o modo operacional da configuração do MetroCluster e efetue uma verificação do MetroCluster.
    a. Confirme a configuração do MetroCluster e se o modo operacional está normal:

    ```
    metrocluster show
    ```

    b. Confirme se todos os nós esperados são mostrados:

    ```
    metrocluster node show
    ```

    c. Emita o seguinte comando:

    ```
    metrocluster check run
    ```

    d. Apresentar os resultados da verificação MetroCluster:

    ```
    metrocluster check show
    ```

14. Se você desativou a criptografia de ponta a ponta antes de adicionar os novos nós, poderá reativá-la seguindo as etapas em "Ative a criptografia de ponta a ponta".
15. Restaure o monitoramento, se necessário, usando o procedimento para sua configuração.

Se você estiver usando…	Use este procedimento
Desempate	"Adição de configurações do MetroCluster" No *MetroCluster Tiebreaker Instalação e Configuração*.

Mediador	"Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster" Em *Instalação e Configuração IP do MetroCluster*.
Aplicativos de terceiros	Consulte a documentação do produto.

16. Para retomar a geração de casos de suporte automático, envie uma mensagem AutoSupport para indicar que a manutenção está concluída.
    a. Emita o seguinte comando:

    ```
    system node autosupport invoke -node * -type all -message MAINT=end
    ```

    b. Repita o comando no cluster de parceiros.

Expanda uma configuração de FC MetroCluster de dois nós para uma configuração de quatro nós

Expansão de uma configuração de FC MetroCluster de dois nós para uma configuração de quatro nós

A expansão de uma configuração de FC MetroCluster de dois nós para uma configuração de FC MetroCluster de quatro nós envolve a adição de uma controladora a cada cluster para formar um par de HA em cada local do MetroCluster e, em seguida, a atualização da configuração de FC MetroCluster.

Antes de começar

- Os nós precisam estar executando o ONTAP 9 ou posterior em uma configuração de MetroCluster FC.

  Este procedimento não é suportado em versões anteriores do ONTAP ou em configurações IP do MetroCluster.

- Se as plataformas em sua configuração de dois nós não forem suportadas no ONTAP 9.2 e você planeja atualizar para plataformas compatíveis com o ONTAP 9.2 *e* expandir para um cluster de quatro nós, você deve atualizar as plataformas na configuração de dois nós *before* expandindo a configuração do MetroCluster FC.
- A configuração existente do MetroCluster FC deve estar correta.
- O equipamento que você está adicionando deve ser suportado e atender a todos os requisitos descritos nos procedimentos a seguir:

  "Instalação e configuração do MetroCluster conectado à malha"

  "Instalação e configuração do Stretch MetroCluster"

- Você precisa ter portas de switch FC disponíveis para acomodar as novas controladoras e todas as novas pontes.
- Verifique se você tem um domínio de broadcast padrão criado nos nós antigos.

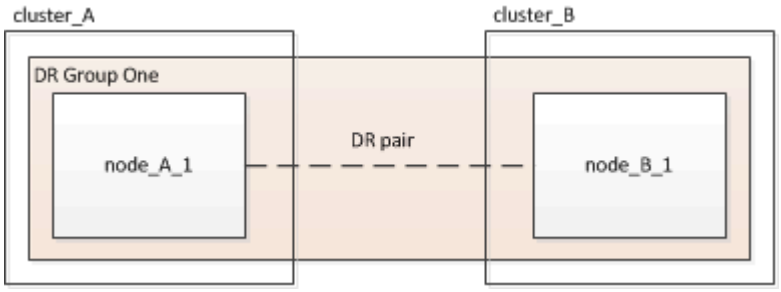
  Quando você adiciona novos nós a um cluster existente sem um domínio de broadcast padrão, as LIFs de

gerenciamento de nós são criadas para os novos nós usando identificadores únicos universais (UUIDs) em vez dos nomes esperados. Para obter mais informações, consulte o artigo da base de dados de Conhecimento "LIFs de gerenciamento de nós em nós recém-adicionados gerados com nomes UUID" .

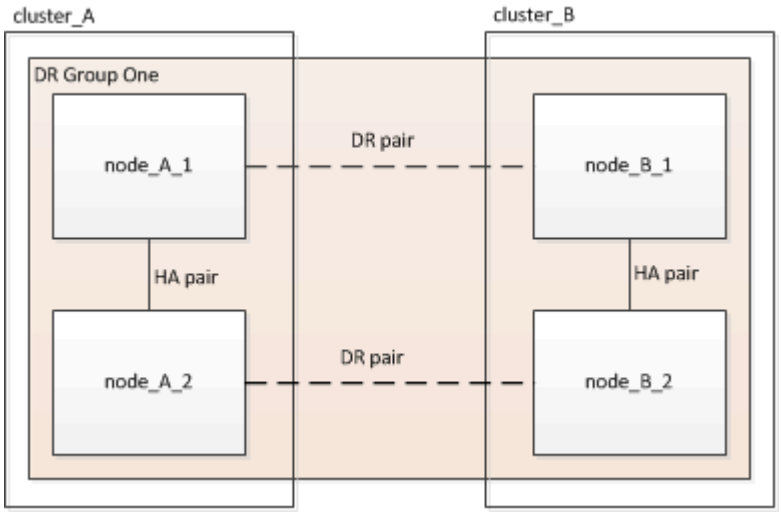
- Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.

Sobre esta tarefa

- Este procedimento aplica-se apenas às configurações do MetroCluster FC.
- Este procedimento é disruptivo e leva aproximadamente quatro horas para ser concluído.
- Antes de executar esse procedimento, a configuração do MetroCluster FC consiste em dois clusters de nó único:



Após concluir este procedimento, a configuração do MetroCluster FC consiste em dois pares de HA, um em cada local:



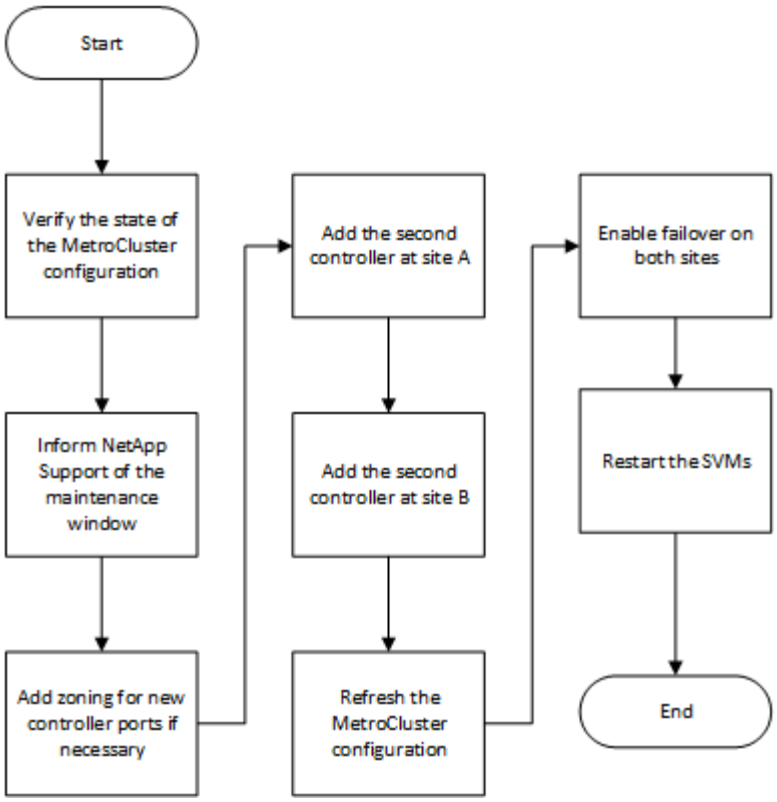
- Ambos os locais devem ser igualmente expandidos.

  Uma configuração do MetroCluster não pode consistir em um número irregular de nós.

- Este procedimento pode demorar mais de uma hora por local, com tempo adicional para tarefas como inicializar os discos e inicializar os novos nós.

  O tempo para inicializar os discos depende do tamanho dos discos.

- Este procedimento utiliza o seguinte fluxo de trabalho:



Ativar o registo da consola

Ative o registo da consola nos seus dispositivos antes de executar esta tarefa.

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Verificando o estado da configuração do MetroCluster

Você deve identificar as controladoras existentes e confirmar as relações de recuperação de desastres (DR) entre elas, se as controladoras estão no modo normal e se os agregados estão espelhados.

Passos

1. Exiba os detalhes dos nós na configuração do MetroCluster a partir de qualquer nó na configuração:

   ```
   metrocluster node show -fields node,dr-partner,dr-partner-systemid
   ```

A saída a seguir mostra que essa configuração do MetroCluster tem um único grupo de DR e um nó em cada cluster.

```
cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
systemid

dr-group-id  cluster         node            dr-partner      dr-partner-
systemid
-----------  -------------   -------         ----------
--------------------
1            cluster_A       controller_A_1  controller_B_1  536946192
1            cluster_B       controller_B_1  controller_A_1  536946165
2 entries were displayed.
```

2. Apresentar o estado da configuração do MetroCluster:

   `metrocluster show`

   A saída a seguir mostra que os nós existentes na configuração MetroCluster estão no modo normal:

```
cluster_A::> metrocluster show

Configuration: two-node-fabric

Cluster                         Entry Name             State
------------------------------ ----------------------
---------------------
Local: cluster_A               Configuration State    configured
                               Mode                   normal
                               AUSO Failure Domain    auso-on-cluster-
disaster
Remote: controller_B_1_siteB
                               Configuration State    configured
                               Mode                   normal
                               AUSO Failure Domain    auso-on-cluster-
disaster
```

3. Verifique o estado dos agregados em cada nó na configuração do MetroCluster:

   `storage aggregate show`

   A saída a seguir mostra que os agregados em cluster_A estão on-line e espelhados:

```
cluster_A::> storage aggregate show


Aggregate                Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

Enviando uma mensagem AutoSupport personalizada antes de adicionar nós à configuração do MetroCluster

Você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Faça login no cluster em Site_A.
2. Chame uma mensagem AutoSupport indicando o início da manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   O `maintenance-window-in-hours` parâmetro especifica o comprimento da janela de manutenção e pode ser um máximo de 72 horas. Se concluir a manutenção antes do tempo decorrido, pode emitir o seguinte comando para indicar que o período de manutenção terminou:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repita esta etapa no site do parceiro.

Zoneamento para as novas portas do controlador ao adicionar um módulo de controlador em uma configuração MetroCluster conetada à malha

O zoneamento do switch FC deve acomodar as novas conexões do controlador. Se você usou os arquivos de configuração de referência (RCFs) fornecidos pelo NetApp para configurar seus switches, o zoneamento é pré-configurado e você não precisa fazer alterações.

Se você configurou manualmente seus switches FC, deve garantir que o zoneamento esteja correto para as conexões do iniciador dos novos módulos do controlador. Consulte as seções sobre zoneamento em "Instalação e configuração do MetroCluster conectado à malha".

Adicione um novo módulo de controlador a cada cluster

Adicionar um novo módulo de controlador a cada cluster

É necessário adicionar um novo módulo de controladora a cada local, criando um par de HA em cada local. Este é um processo de várias etapas envolvendo alterações de hardware e software que devem ser realizadas na ordem correta em cada local.

Sobre esta tarefa

- O novo módulo do controlador deve ser recebido da NetApp como parte do kit de atualização.

  Você deve verificar se as placas PCIe no novo módulo de controladora são compatíveis e suportadas pelo novo módulo de controladora.

  "NetApp Hardware Universe"

- O sistema precisa ter um slot vazio disponível para o novo módulo de controladora ao fazer a atualização para um par de HA de chassi único (um par de HA no qual ambos os módulos de controladora residem no mesmo chassi).

  Esta configuração não é suportada em todos os sistemas. As plataformas com configurações de chassi único compatíveis com ONTAP 9 são AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080 e FAS9000.

- É necessário ter espaço em rack e cabos para o novo módulo de controladora ao fazer a atualização para um par de HA de chassi duplo (um par de HA no qual os módulos da controladora residem em chassi separado).

  Esta configuração não é suportada em todos os sistemas.

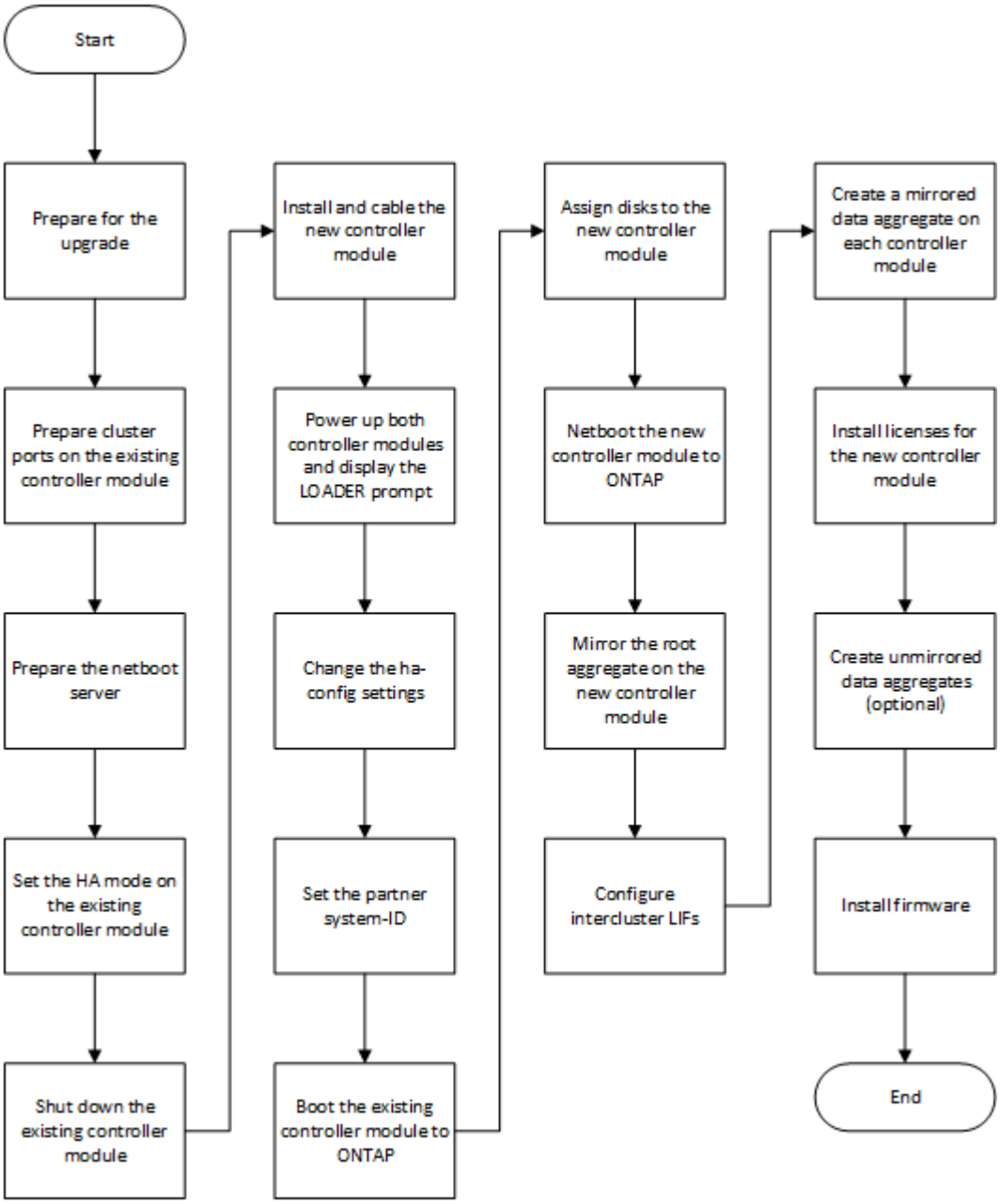
- Você deve conetar cada módulo do controlador à rede de gerenciamento por meio de sua porta e0a ou, se o sistema tiver uma, você pode se conetar à porta e0M como a porta de gerenciamento.
- Essas tarefas devem ser repetidas em cada local.
- Os módulos do controlador pré-existentes são referidos como módulos do controlador *existing*.

  Os exemplos deste procedimento têm o prompt do console `existing_ctlr>` .

- Os módulos do controlador que estão sendo adicionados são chamados de módulos do controlador *new*;

os exemplos deste procedimento têm o prompt do console `new_ctlr>` .

- Esta tarefa utiliza o seguinte fluxo de trabalho:



Preparando-se para a atualização

Antes de atualizar para um par de HA, verifique se o sistema atende a todos os requisitos e se tem todas as informações necessárias.

Passos

1. Identifique discos não atribuídos ou discos sobressalentes que você pode atribuir ao novo módulo de controladora usando os seguintes comandos:
   - `storage disk show -container-type spare`
   - `storage disk show -container-type unassigned`

2. Conclua as seguintes subetapas:
   a. Determine onde os agregados para o nó existente estão localizados:

      ```
      storage aggregate show
      ```

   b. Se a atribuição automática de propriedade de disco estiver ativada, desative-a:

      ```
      storage disk option modify -node node_name -autoassign off
      ```

   c. Remova a propriedade em discos que não têm agregados neles:

      ```
      storage disk removeowner disk_name
      ```

   d. Repita a etapa anterior para quantos discos forem necessários para o novo nó.
3. Verifique se você tem cabos prontos para as seguintes conexões:
   - Conexões de cluster

     Se você estiver criando um cluster sem switch de dois nós, precisará de dois cabos para conetar os módulos do controlador. Caso contrário, você precisa de um mínimo de quatro cabos, dois para cada conexão de módulo de controlador ao switch de cluster-rede. Outros sistemas (como a série 80xx) têm padrões de quatro ou seis conexões de cluster.

   - Conexões de INTERCONEXÃO HA, se o sistema estiver em um par de HA de chassi duplo
4. Verifique se você tem um console de porta serial disponível para os módulos do controlador.
5. Verifique se seu ambiente atende aos requisitos do local e do sistema.

   "NetApp Hardware Universe"

6. Reúna todos os endereços IP e outros parâmetros de rede para o novo módulo do controlador.

Limpando a configuração em um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   ```
   halt
   ```

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

   ```
   set-defaults
   ```

3. Salvar o ambiente:

   ```
   saveenv
   ```

4. No prompt DO Loader, inicie o menu de inicialização:

   ```
   boot_ontap menu
   ```

5. No prompt do menu de inicialização, desmarque a configuração:

   `wipeconfig`

   Responda `yes` ao prompt de confirmação.

   O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

   Responda `yes` ao prompt de confirmação.

Preparando portas do cluster em um módulo do controlador existente

Antes de instalar um novo módulo de controlador, tem de configurar as portas do cluster no módulo de controlador existente para que as portas do cluster possam fornecer comunicação do cluster com o novo módulo de controlador.

Sobre esta tarefa

Se estiver criando um cluster de dois nós (sem switches de rede de cluster), você deverá ativar o modo de rede sem switch de cluster.

Para obter informações detalhadas sobre a configuração de porta, LIF e rede no ONTAP, "Gerenciamento de rede"consulte .

Passos

1. Determine quais portas devem ser usadas como portas de cluster do nó.

   Para obter uma lista das funções de porta padrão da sua plataforma, consulte a. "Hardware Universe"

   As *instruções de instalação e configuração* da sua plataforma no site de suporte da NetApp contém informações sobre as portas para conexões de rede de cluster.

2. Para cada porta de cluster, identifique as funções de porta:

   `network port show`

   No exemplo a seguir, os portos "'e0a'", "'e0b'", "'e0c'" e "'e0d" devem ser alterados para portas de cluster:

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. Para qualquer LIF de dados que esteja usando uma porta de cluster como porta inicial ou porta atual, modifique o LIF para usar uma porta de dados como porta inicial:

   `network interface modify`

   O exemplo a seguir altera a porta inicial de um LIF de dados para uma porta de dados:

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. Para cada LIF que você modificou, reverta o LIF para sua nova porta inicial:

   `network interface revert`

   O exemplo a seguir reverte o LIF "d.atalif1" para sua nova porta inicial "'e1b":

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Remova quaisquer portas VLAN usando portas de cluster como portas membro e ifgrps usando portas de cluster como portas membro.

   a. Excluir portas VLAN
      `network port vlan delete -node *node-name* -vlan-name *portid-vlandid*`

Por exemplo:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remover portas físicas dos grupos de interface:

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Por exemplo:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Remover portas VLAN e grupo de interfaces do domínio de broadcast::

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modifique as portas do grupo de interfaces para usar outras portas físicas como membro, conforme necessário
`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

6. Verifique se as funções de porta foram alteradas:

`network port show`

O exemplo a seguir mostra que as portas "'e0a"", "'e0b"", "'e0c" e "'e0d" são agora portas de cluster:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Adicione as portas ao domínio de broadcast do cluster:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id`*`,` *`port-id`*`,` *`port-id`*`…`

   Por exemplo:

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. Se o sistema fizer parte de um cluster comutado, crie LIFs de cluster nas portas do cluster: `network interface create`

   O exemplo a seguir cria um LIF de cluster em uma das portas de cluster do nó. O `-auto` parâmetro configura o LIF para usar um endereço IP local de link.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. Se você estiver criando um cluster sem switch de dois nós, ative o modo de rede sem switch de cluster:

   a. Altere para o nível de privilégio avançado de qualquer nó:

      `set -privilege advanced`

Você pode responder `y` quando solicitado se deseja continuar no modo avançado. O prompt do modo avançado é (`*>`exibido).

a. Ative o modo de rede do cluster sem switch:

```
network options switchless-cluster modify -enabled true
```

b. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

> A criação da interface do cluster para o nó existente em um sistema de cluster sem switch de dois nós é concluída após a instalação do cluster ser concluída por meio de um netboot no novo módulo do controlador.

Preparando o servidor netboot para baixar a imagem

Quando estiver pronto para preparar o servidor netboot, você deve baixar a imagem correta do ONTAP netboot do site de suporte da NetApp para o servidor netboot e anotar o endereço IP.

Sobre esta tarefa

- Você deve ser capaz de acessar um servidor HTTP do sistema antes e depois de adicionar o novo módulo de controlador.
- Você deve ter acesso ao site de suporte da NetApp para baixar os arquivos de sistema necessários para sua plataforma e sua versão do ONTAP.

  "Site de suporte da NetApp"

- Ambos os módulos de controladora no par de HA devem executar a mesma versão do ONTAP.

Passos

1. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o `<ontap_version>_image.tgz` ficheiro num diretório acessível pela Web.

   O `<ontap_version>_image.tgz` arquivo é usado para executar uma netboot do seu sistema.

2. Mude para o diretório acessível pela Web e verifique se os arquivos necessários estão disponíveis.

Para…	Então…

Sistemas das séries FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	Extraia o conteúdo do arquivo ONTAP_version>_image.tgz para o diretório de destino: `tar -zxvf <ontap_version>_image.tgz` Se você estiver extraindo o conteúdo no Windows, use 7-Zip ou WinRAR para extrair a imagem netboot. Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel: `netboot/kernel`
Todos os outros sistemas	Sua lista de diretórios deve conter o seguinte arquivo: `<ontap_version>_image.tgz` Não há necessidade de extrair o conteúdo do arquivo.

3. Determine o endereço IP do módulo do controlador existente.

   Este endereço é referido posteriormente neste procedimento *ip-address-of-existing controller* como .

4. Ping *ip-address-of-existing controller* para verificar se o endereço IP está acessível.

Definir o modo HA no módulo do controlador existente

Você deve usar o comando storage failover modify para definir o modo no módulo de controladora existente. O valor do modo é ativado mais tarde, depois de reiniciar o módulo do controlador.

Passos

1. Defina o modo como HA:

   `storage failover modify -mode ha -node existing_node_name`

Encerrar o módulo de controladora existente

Você deve executar um desligamento normal do módulo do controlador existente para verificar se todos os dados foram gravados no disco. Também tem de desligar as fontes de alimentação.

Sobre esta tarefa

Você deve executar um desligamento normal do sistema antes de substituir os componentes do sistema para evitar a perda de dados não gravados no NVRAM ou no NVMEM.

Passos

1. Interrompa o nó do prompt do módulo de controladora existente:

   ```
   halt local -inhibit-takeover true
   ```

   Se você for solicitado a continuar o procedimento de parada, digite `y` quando solicitado e aguarde até que o sistema pare no prompt DO Loader.

   Em um sistema 80xx, o LED NVRAM está localizado no módulo do controlador à direita das portas de rede, marcado com um símbolo de bateria.

   Este LED fica intermitente se existirem dados não gravados no NVRAM. Se este LED estiver piscando em âmbar depois de inserir o comando halt, você precisará reiniciar o sistema e tentar interrompê-lo novamente.

2. Se você ainda não está aterrado, aterre-se adequadamente.
3. Desligue as fontes de alimentação e desligue a alimentação, utilizando o método correto para o seu sistema e tipo de fonte de alimentação:

Se o seu sistema utilizar…	Então…
Fontes de alimentação CA	Desconete os cabos de energia da fonte de alimentação e remova-os.
Fontes de alimentação CC	Retire a alimentação da fonte de CC e, em seguida, retire os fios DC, se necessário.

Instale e faça o cabo do novo módulo do controlador

Instalação e cabeamento do novo módulo de controladora

Você deve instalar fisicamente o novo módulo do controlador no chassi e, em seguida, fazer o cabo.

Passos

1. Se você tiver um módulo de expansão de e/S (IOXM) em seu sistema e estiver criando um par de HA de chassi único, será necessário desvincular e remover o IOXM.

   Em seguida, você pode usar o compartimento vazio para o novo módulo do controlador. No entanto, a nova configuração não terá a e/S extra fornecida pelo IOXM.

2. Instale fisicamente o novo módulo do controlador e, se necessário, instale ventoinhas adicionais:

Se você estiver adicionando um módulo de controlador…	Em seguida, execute estas etapas…

Para um compartimento vazio para criar um par de HA de chassi único e o sistema pertence a uma das seguintes plataformas:	a. Remova a placa vazia na parte traseira do chassi que cobre o compartimento vazio que conterá o novo módulo do controlador. b. Empurre cuidadosamente o módulo do controlador até meio para dentro do chassis. Para evitar que o módulo do controlador inicialize automaticamente, não o coloque totalmente no chassis até mais tarde neste procedimento.
Em um chassi separado de seu parceiro de HA para criar um par de HA de chassi duplo quando a configuração existente estiver em uma configuração de módulo IOX-controlador. • FAS8200 • 80xx	Instale o novo sistema no rack ou no gabinete do sistema.

3. Faça o cabeamento das conexões de rede do cluster, conforme necessário:

   a. Identifique as portas no módulo do controlador para as ligações do cluster.

      "Sistemas AFF A320: Instalação e configuração"

      "Instruções de instalação e configuração dos sistemas AFF A220/FAS2700"

      "Instruções de instalação e configuração de sistemas AFF A800"

      "Instruções de instalação e configuração de sistemas AFF A300"

      "Instruções de instalação e configuração de sistemas FAS8200"

   b. Se você estiver configurando um cluster comutado, identifique as portas que você usará nos switches de rede do cluster.

      Consulte "Guia de configuração de switch Data ONTAP em cluster para switches Cisco" "Guia de instalação do interrutor de modo de cluster do NetApp 10G" , ou "Guia de instalação do comutador de modo de cluster do NetApp 1G", dependendo dos interrutores que estiver a utilizar.

   c. Conete os cabos às portas do cluster:

Se o cluster for…	Então…
Um cluster sem switch de dois nós	Conete diretamente as portas do cluster no módulo do controlador existente às portas do cluster correspondentes no novo módulo do controlador.
Um cluster comutado	Conete as portas do cluster em cada controlador às portas nos switches de rede do cluster identificados na subetapa b.

Faça o cabeamento das portas FC-VI e HBA do novo módulo de controladora aos switches FC

As portas FC-VI e HBAs (adaptadores de barramento do host) do novo módulo de controladora devem ser cabeadas para os switches FC do local.

Passos

1. Faça o cabeamento das portas FC-VI e das portas HBA, usando a tabela para sua configuração e modelo de switch.
   - "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"
   - "Atribuições de portas para sistemas que usam duas portas de iniciador"

Cabeamento das conexões de peering de cluster do novo módulo de controladora

Você deve enviar o novo módulo de controladora à rede de peering de cluster para que ele tenha conetividade com o cluster no site do parceiro.

Sobre esta tarefa

Pelo menos duas portas em cada módulo de controlador devem ser usadas para peering de cluster.

A largura de banda mínima recomendada para as portas e a conetividade de rede é de 1 GbE.

Passos

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conetividade de rede com o cluster do parceiro.

Ligar ambos os módulos do controlador e apresentar o aviso Loader

Você liga o módulo do controlador existente e o novo módulo do controlador para exibir o prompt Loader.

Passos

Ligue os módulos do controlador e interrompa o processo de arranque, seguindo os passos para a sua configuração:

Se os módulos do controlador forem…	Então…

No mesmo chassi	1. Verifique se o novo módulo do controlador está **não** totalmente inserido no compartimento. O módulo do controlador existente deve ser totalmente inserido no compartimento porque nunca foi removido do chassi, mas o novo módulo do controlador não deve ser. 2. Ligue a alimentação e ligue as fontes de alimentação para que o módulo do controlador existente receba energia. 3. Interrompa o processo de inicialização no módulo do controlador existente pressionando Ctrl-C. 4. Empurre firmemente o novo módulo do controlador para dentro do compartimento. Quando totalmente sentado, o novo módulo do controlador recebe alimentação e arranca automaticamente. 5. Interrompa o processo de inicialização pressionando Ctrl-C. 6. Aperte o parafuso de aperto manual na pega do excêntrico, se presente. 7. Instale o dispositivo de gerenciamento de cabos, se houver. 8. Prenda os cabos ao dispositivo de gerenciamento de cabos com o gancho e a alça de loop.
Em chassis separado	1. Ligue as fontes de alimentação no módulo do controlador existente. 2. Interrompa o processo de inicialização pressionando Ctrl-C. 3. Repita estes passos para o novo módulo do controlador

Cada módulo do controlador deve exibir o prompt Loader (`LOADER>`, , `LOADER-A>` ou `LOADER-B>`).

Se não houver nenhum prompt DO Loader, Registre a mensagem de erro. Se o sistema exibir o menu de inicialização, reinicie e tente interromper o processo de inicialização novamente.

Alterar a configuração ha-config nos módulos de controladora existentes e novos

Ao expandir uma configuração do MetroCluster, você deve atualizar a configuração ha-config do módulo de controladora existente e do novo módulo de controladora. Você também deve determinar a ID do sistema do novo módulo do controlador.

Sobre esta tarefa

Esta tarefa é executada no modo Manutenção nos módulos do controlador existentes e novos.

Passos

1. Altere a configuração ha-config do módulo controlador existente:

   a. Exiba a configuração ha-config do módulo de controladora e do chassi existentes:

      ```
      ha-config show
      ```

A configuração ha-config é "mcc-2n" para todos os componentes porque o módulo controlador estava em uma configuração MetroCluster de dois nós.

b. Altere a configuração ha-config do módulo controlador existente para "mcc"
`ha-config modify controller mcc`

c. Altere a configuração ha-config do chassi existente para "mcc":

```
ha-config modify chassis mcc
```

d. Recupere a ID do sistema para o módulo do controlador existente:

```
sysconfig
```

Anote a ID do sistema. Você precisa dele quando você definir o ID do parceiro no novo módulo do controlador.

a. Saia do modo de manutenção para retornar ao prompt Loader:

```
halt
```

2. Altere a configuração ha-config e recupere a ID do sistema do novo módulo do controlador:

a. Se o novo módulo do controlador ainda não estiver no modo de manutenção, inicie-o no modo de manutenção:

```
boot_ontap maint
```

b. Altere a configuração ha-config do novo módulo de controlador para "mcc":

```
ha-config modify controller mcc
```

c. Altere a configuração ha-config do novo chassi para mcc:

```
ha-config modify chassis mcc
```

d. Recupere a ID do sistema para o novo módulo do controlador:

```
sysconfig
```

Anote a ID do sistema. Você precisa dele quando você definir o ID do parceiro e atribuir discos ao novo módulo do controlador.

a. Saia do modo de manutenção para retornar ao prompt Loader:

```
halt
```

Definir a ID do sistema do parceiro para ambos os módulos do controlador

Você precisa definir o ID do sistema do parceiro em ambos os módulos da controladora para que eles possam formar um par de HA.

Sobre esta tarefa

Esta tarefa é executada com ambos os módulos do controlador no prompt Loader.

Passos

1. No módulo do controlador existente, defina a ID do sistema do parceiro para a ID do novo módulo do controlador:

   `setenv partner-sysid *sysID_of_new_controller*`

2. No novo módulo do controlador, defina a ID do sistema do parceiro para a ID do módulo do controlador existente:

   `setenv partner-sysid *sysID_of_existing_controller*`

Inicializando o módulo controlador existente

Você deve inicializar o módulo de controladora existente no ONTAP.

Passos

1. No prompt DO Loader, inicialize o módulo do controlador existente no ONTAP:

   `boot_ontap`

Atribuindo discos ao novo módulo do controlador

Antes de concluir a configuração do novo módulo de controladora através do netboot, você deve atribuir discos a ele.

Sobre esta tarefa

Você precisa ter certeza de que há peças sobressalentes, discos não atribuídos ou discos atribuídos suficientes que não façam parte de um agregado existente.

"Preparando-se para a atualização"

Estas etapas são executadas no módulo do controlador existente.

Passos

1. Atribua o disco raiz ao novo módulo do controlador:

   `storage disk assign -disk *disk_name* -sysid *new_controller_sysID* -force true`

   Se o modelo da plataforma usar o recurso Advanced Drive Partitioning (ADP), você deve incluir o parâmetro -root True:

   `storage disk assign -disk *disk_name* -root true -sysid *new_controller_sysID* -force true`

2. Atribua os restantes discos necessários ao novo módulo do controlador introduzindo o seguinte comando para cada disco:

   `storage disk assign -disk *disk_name* -sysid *new_controller_sysID* -force true`

3. Verifique se as atribuições de disco estão corretas:

   `storage disk show -partitionownership*`

Certifique-se de que atribuiu todos os discos que pretende atribuir ao novo nó.

Netbooting e configuração de ONTAP no novo módulo de controlador

Você deve executar uma sequência específica de etapas para netboot e instalar o sistema operacional ONTAP no novo módulo do controlador ao adicionar módulos do controlador a uma configuração existente do MetroCluster.

Sobre esta tarefa

- Esta tarefa é iniciada no prompt Loader do novo módulo do controlador.
- Esta tarefa inclui a inicialização de discos.

  O tempo necessário para inicializar os discos depende do tamanho dos discos.

- O sistema atribui automaticamente dois discos ao novo módulo do controlador.

  "Gerenciamento de disco e agregado"

Passos

1. No prompt DO Loader, configure o endereço IP do novo módulo do controlador com base na disponibilidade do DHCP:

Se DHCP for…	Em seguida, digite o seguinte comando…
Disponível	**`ifconfig e0M -auto`**
Não disponível	`ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* É o endereço IP do sistema de armazenamento. *`netmask`* é a máscara de rede do sistema de armazenamento. *`gateway`* é o gateway para o sistema de armazenamento. *`dns_addr`* É o endereço IP de um servidor de nomes na rede. *`dns_domain`* É o nome de domínio do sistema de nomes de domínio (DNS). Se você usar esse parâmetro opcional, não precisará de um nome de domínio totalmente qualificado no URL do servidor netboot; você precisará apenas do nome de host do servidor. Outros parâmetros podem ser necessários para sua interface. Para obter detalhes, use o `help ifconfig` comando no prompt DO Loader.

2. No prompt Loader, netboot o novo nó:

Para…	Emitir este comando…
Sistemas das séries FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Todos os outros sistemas	`netboot \http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

O *path_to_the_web-accessible_directory* é a localização do ficheiro transferido `<ontap_version>_image.tgz`.

3. Selecione a opção **Instalar novo software primeiro** no menu exibido.

   Esta opção de menu transfere e instala a nova imagem ONTAP no dispositivo de arranque.

   - Você deve digitar "'y'" quando solicitado com a mensagem de que este procedimento não é compatível para atualização sem interrupções em um par de HA.
   - Você deve inserir "'y'" quando avisado que esse processo substitui o software ONTAP existente por um novo software.
   - Você deve inserir o caminho da seguinte forma quando solicitado para o URL do arquivo image.tgz:

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Digite "'y'" quando solicitado a respeito de atualização sem interrupções ou substituição do software.
5. Insira o caminho para o arquivo image.tgz quando solicitado para o URL do pacote.

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. Digite "'n'" para ignorar a recuperação de backup quando solicitado a restaurar a configuração de backup.

```
*************************************************************
*             Restore Backup Configuration                  *
*  This procedure only applies to storage controllers that  *
*  are configured as an HA pair.                            *
*                                                           *
*  Choose Yes to restore the "varfs" backup configuration   *
*  from the SSH server.  Refer to the Boot Device Replacement *
*  guide for more details.                                  *
*  Choose No to skip the backup recovery and return to the  *
*  boot menu.                                               *
*************************************************************

Do you want to restore the backup configuration
now? {y|n} `n`
```

7. Digite "'y'" quando solicitado a reinicializar agora.

```
The node must be rebooted to start using the newly installed software.
Do you want to
reboot now? {y|n} `y`
```

8. Se necessário, selecione a opção **Limpar configuração e inicializar todos os discos** após o nó ter inicializado.

   Como você está configurando um novo módulo de controlador e os discos do novo módulo de controlador estão vazios, você pode responder "y" quando o sistema avisa que isso apagará todos os discos.

   ⓘ O tempo necessário para inicializar os discos depende do tamanho dos discos e da configuração.

9. Depois que os discos forem inicializados e o assistente Configuração de cluster for iniciado, configure o nó:

   Insira as informações de LIF de gerenciamento de nós no console.

10. Faça login no nó, insira o `cluster setup` e, em seguida, digite "'join'" quando solicitado a ingressar no cluster.

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

11. Responda aos prompts restantes, conforme apropriado para o seu site.

    O "Configuração do ONTAP" para a sua versão do ONTAP contém detalhes adicionais.

12. Se o sistema estiver em uma configuração de cluster sem switch de dois nós, crie as interfaces de cluster

no nó existente usando o comando Create de interface de rede para criar LIFs de cluster nas portas do cluster.

A seguir está um exemplo de comando para criar um cluster LIF em uma das portas de cluster do nó. O parâmetro -auto configura o LIF para usar um endereço IP local de link.

```
cluster_A::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node_A_1 -home-port e1a -auto true
```

13. Após a conclusão da configuração, verifique se o nó está íntegro e qualificado para participar do cluster:

    `cluster show`

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

```
cluster_A::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node_A_1              true    true
node_A_2              true    true
```

    Você pode acessar o assistente Configuração de cluster para alterar qualquer um dos valores inseridos para a máquina virtual de armazenamento de administrador (SVM) ou nó SVM usando o comando de configuração de cluster.

14. Confirme se você tem quatro portas configuradas como interconexões de cluster:

    `network port show`

    O exemplo a seguir mostra a saída para dois módulos de controlador em cluster_A:

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

Espelhamento do agregado de raiz na nova controladora

Você precisa espelhar o agregado raiz para fornecer proteção de dados ao adicionar um controlador a uma configuração do MetroCluster.

Esta tarefa deve ser executada no novo módulo do controlador.

1. Espelhar o agregado raiz:

   `storage aggregate mirror` *`aggr_name`*

   O comando a seguir espelha o agregado raiz para controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Isso reflete o agregado, por isso consiste em um Plex local e um Plex remoto localizado no local remoto de MetroCluster.

Configurar LIFs entre clusters

Saiba como configurar LIFs entre clusters em portas dedicadas e compartilhadas.

Configurar LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas para aumentar a largura de banda disponível para tráfego de replicação.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que as portas "e0e" e "e0f" não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

   `network interface failover-groups create -vserver <system_SVM> -failover -group <failover_group> -targets <physical_or_logical_ports>`

   O exemplo a seguir atribui as portas "e0e" e "e0f" ao grupo de failover "intercluster01" no SVM do sistema "cluster01":

```
cluster01::> network interface failover-groups create -vserver
cluster01 -failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

   `network interface failover-groups show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-
01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-
01:e0d,
                                  cluster01-02:e0c, cluster01-
02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Versão de ONTAP	Comando
9,6 e mais tarde	`network interface create -vserver <system_SVM> -lif <LIF_name> -service-policy default-intercluster -home -node <node> -home-port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`
9,5 e anteriores	`network interface create -vserver system_SVM -lif <LIF_name> -role intercluster -home-node <node> -home -port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" no grupo de failover "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

Em ONTAP 9.6 e posteriores:
`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:
`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. Verifique se as LIFs entre clusters são redundantes:

Em ONTAP 9.6 e posteriores:

```
network interface show -service-policy default-intercluster -failover
```

Em ONTAP 9.5 e anteriores:

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta SVM "e0e" falharão para a porta "e0f".

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados para reduzir o número de portas necessárias para a rede entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
```

2. Criar LIFs entre clusters no sistema:

Em ONTAP 9.6 e posteriores:
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
Em ONTAP 9.5 e anteriores:
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

Em ONTAP 9.6 e posteriores:
`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:
`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. Verifique se as LIFs entre clusters são redundantes:

Em ONTAP 9.6 e posteriores:

```
network interface show –service-policy default-intercluster -failover
```

Em ONTAP 9.5 e anteriores:

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "e0c" falharão para a porta "e0d".

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

Sobre esta tarefa

- Você deve saber quais unidades serão usadas no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.
- As unidades são de propriedade de um nó específico; quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.

  Em sistemas que usam ADP, agregados são criados usando partições nas quais cada unidade é particionada em partições P1, P2 e P3.

- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.

  "Gerenciamento de disco e agregado"

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

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   `storage disk show -spare -owner node_name`

2. Criar o agregado:

   `storage aggregate create -mirror true`

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para garantir que o agregado seja criado em um nó específico, use o `-node` parâmetro ou especifique as unidades que são de propriedade desse nó.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas que devem ser adicionadas ao agregado
   - Número de unidades a incluir

     Na configuração mínima suportada, na qual um número limitado de unidades está disponível, você deve usar a opção force-small-Aggregate para permitir a criação de um agregado RAID-DP de três discos.

   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades que podem ser incluídas em um grupo RAID
   - Se unidades com RPM diferentes são permitidas

     Para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

     O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate aggregate-name`

Instalar licenças para o novo módulo de controlador

É necessário adicionar licenças para o novo módulo de controladora para quaisquer serviços ONTAP que exijam licenças padrão (node-locked). Para recursos com licenças padrão, cada nó no cluster deve ter sua própria chave para o recurso.

Para obter informações detalhadas sobre licenciamento, consulte o artigo 3013749 da base de conhecimento: Visão geral e referências de licenciamento do Data ONTAP 8.2 no site de suporte da NetApp e na *Referência de administração do sistema*.

Passos

1. Se necessário, obtenha chaves de licença para o novo nó no site de suporte da NetApp na seção meu suporte em licenças de software.

   Para obter mais informações sobre substituições de licenças, consulte o artigo da base de dados de Conhecimento "Pós-processo de substituição da placa-mãe para atualizar o licenciamento em um sistema AFF/FAS."

2. Execute o seguinte comando para instalar cada chave de licença:

   `system license add -license-code license_key`

   O *license_key* tem 28 dígitos de comprimento.

3. Repita este passo para cada licença padrão (node-locked) necessária.

Criação de agregados de dados sem espelhamento

Você pode, opcionalmente, criar agregados de dados sem espelhamento para dados que não exigem o espelhamento redundante fornecido pelas configurações do MetroCluster.

Sobre esta tarefa

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode verificar se o tipo de unidade correto está selecionado.

> Nas configurações IP do MetroCluster, agregados remotos sem espelhamento não são acessíveis após um switchover

Os agregados sem espelhamento devem ser locais para o nó que os possui.

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.
- *Gerenciamento de discos e agregados* contém mais informações sobre o espelhamento de agregados.

Passos

1. Instale e faça o cabeamento das gavetas de disco que conterão os agregados sem espelhamento.

   Você pode usar os procedimentos na documentação *Instalação e Configuração* para sua plataforma e prateleiras de disco.

   "Documentação dos sistemas de hardware da ONTAP"

2. Atribua manualmente todos os discos na nova gaveta ao nó apropriado:

   ```
   disk assign -disk <disk-id> -owner <owner-node-name>
   ```

3. Criar o agregado:

   ```
   storage aggregate create
   ```

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para verificar se o agregado é criado em um nó específico, você deve usar o `-node` parâmetro ou especificar unidades que são de propriedade desse nó.

   Verifique se você está incluindo apenas unidades na gaveta sem espelhamento para o agregado.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas ou LUNs de storage que devem ser adicionados ao agregado
   - Número de unidades a incluir
   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
   - Se unidades com RPM diferentes são permitidas

     Para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

     O comando a seguir cria um agregado sem espelhamento com 10 discos:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

+

Você também pode usar o `-disklist` parâmetro no comando para especificar os discos que deseja usar para o agregado.

4. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate <aggregate-name>`

Informações relacionadas

"Gerenciamento de disco e agregado"

Instalar o firmware depois de adicionar um módulo de controlador

Depois de adicionar o módulo do controlador, tem de instalar o firmware mais recente no novo módulo do controlador para que o módulo do controlador funcione corretamente com o ONTAP.

Passos

1. Transfira a versão mais atual do firmware para o seu sistema e siga as instruções para transferir e instalar o novo firmware.

   "Downloads do NetApp: Firmware e Diagnóstico do sistema"

Atualizando a configuração do MetroCluster com novos controladores

É necessário atualizar a configuração do MetroCluster ao expandi-la de uma configuração de dois nós para uma configuração de quatro nós.

Passos

1. Atualize a configuração do MetroCluster:

   a. Entre no modo de privilégio avançado
   `set -privilege advanced`

   b. Atualize a configuração do MetroCluster
   `metrocluster configure -refresh true -allow-with-one-aggregate true`

   O comando a seguir atualiza a configuração do MetroCluster em todos os nós do grupo DR que contém controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

a. Voltar ao modo de privilégios de administrador:

```
set -privilege admin
```

2. Verifique o status da rede no local A:

```
network port show
```

O exemplo a seguir mostra o uso da porta de rede em uma configuração MetroCluster de quatro nós:

```
cluster_A::> network port show
                                                                 Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.

a. Verifique a configuração do local A:

```
metrocluster show
```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Verifique a configuração a partir do local B:

`metrocluster show`

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

c. Verifique se as relações de DR foram criadas corretamente:

`metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner`

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Ativação do failover de storage nos módulos da controladora e ativação da HA do cluster

Depois de adicionar novos módulos de controladora à configuração do MetroCluster, você deve habilitar o failover de storage nos dois módulos de controladora e ativar separadamente a HA do cluster.

Antes de começar

A configuração do MetroCluster deve ter sido atualizada anteriormente usando o `metrocluster configure -refresh true` comando.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Ativar failover de storage:

   `storage failover modify -enabled true -node` *`existing-node-name`*

   O único comando permite o failover de armazenamento em ambos os módulos da controladora.

2. Verifique se o failover de armazenamento está ativado:

   `storage failover show`

   A saída deve ser semelhante ao seguinte:

```
Node           Partner        Possible State Description
-------------- -------------- -------- ---------------------
old-ctlr        new-ctlr      true      Connected to new-ctlr
new-ctlr        old-ctlr      true      Connected to old-ctlr
2 entries were displayed.
```

3. Ativar cluster HA:

   ```
   cluster ha modify -configured true
   ```

   A alta disponibilidade do cluster (HA) deve ser configurada em um cluster se ele contiver apenas dois nós e for diferente da HA fornecida pelo failover de storage.

Reiniciando os SVMs

Depois de expandir a configuração do MetroCluster, você deve reiniciar os SVMs.

Passos

1. Identificar os SVMs que precisam ser reiniciados:

   ```
   metrocluster vserver show
   ```

   Este comando mostra os SVMs em ambos os clusters MetroCluster.

2. Reinicie os SVMs no primeiro cluster:
   a. Entre no modo de privilégio avançado, pressionando **y** quando solicitado:

      ```
      set -privilege advanced
      ```

   b. Reinicie as SVMs:

      ```
      vserver start -vserver SVM_name -force true
      ```

   c. Voltar ao modo de privilégios de administrador:

      ```
      set -privilege admin
      ```

3. Repita a etapa anterior no cluster de parceiros.
4. Verifique se os SVMs estão em um estado saudável:

   ```
   metrocluster vserver show
   ```

Expanda uma configuração de FC MetroCluster de quatro nós para uma configuração de oito nós

Expansão de uma configuração de FC MetroCluster de quatro nós para uma configuração de oito nós

A expansão de uma configuração de FC MetroCluster de quatro nós para uma configuração de FC MetroCluster de oito nós envolve a adição de duas controladoras a cada cluster para formar um segundo par de HA em cada local do MetroCluster e a execução da operação de configuração de FC do MetroCluster.

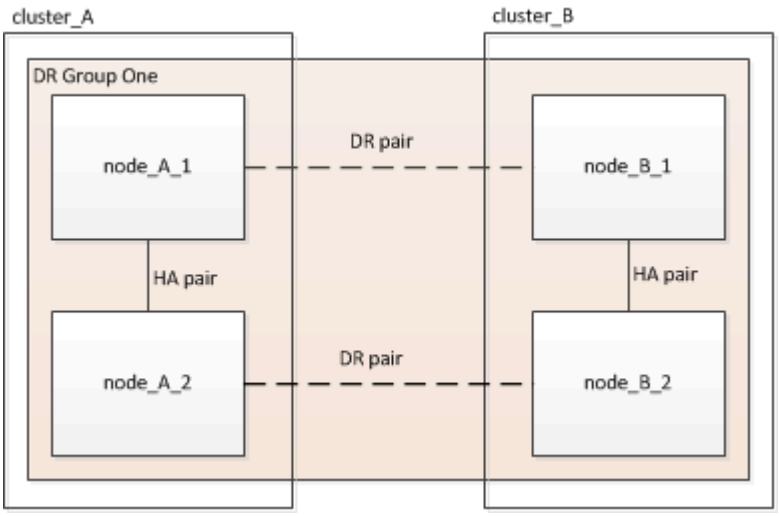
Sobre esta tarefa

- Os nós precisam estar executando o ONTAP 9 em uma configuração de MetroCluster FC.

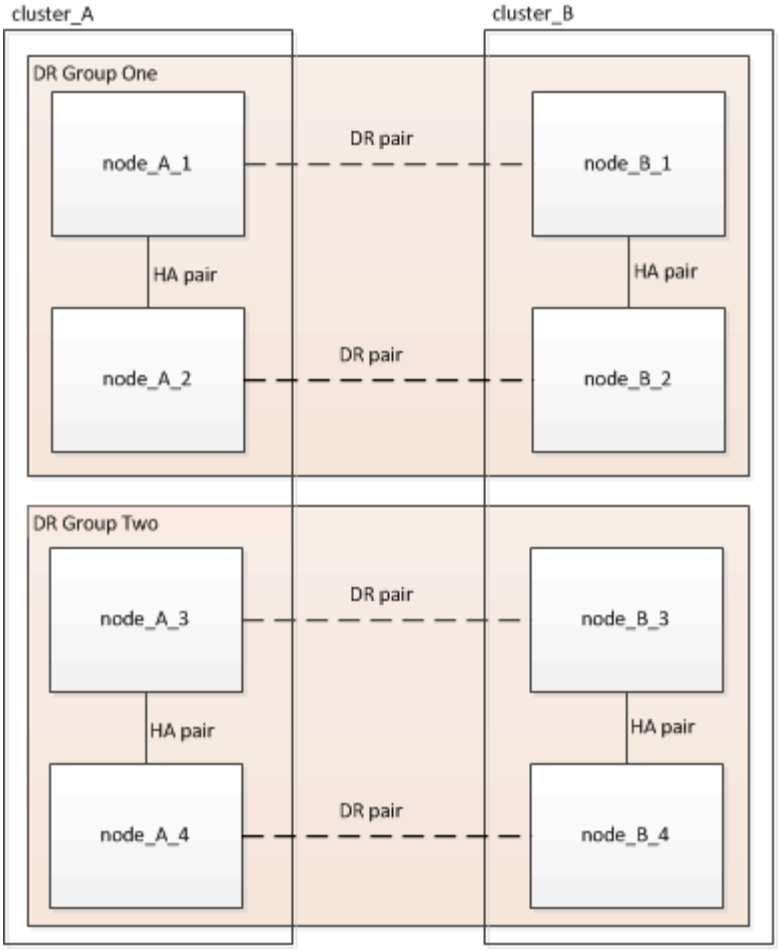
  Este procedimento não é suportado em versões anteriores do ONTAP ou em configurações IP do MetroCluster.

- A configuração existente do MetroCluster FC deve estar correta.
- O equipamento que está a adicionar tem de ser suportado e cumprir todos os requisitos descritos em "Instalação e configuração do MetroCluster conectado à malha"
- Você precisa ter portas de switch FC disponíveis para acomodar as novas controladoras e todas as novas pontes.
- Você precisa da senha de administrador e acesso a um servidor FTP ou SCP.
- Este procedimento aplica-se apenas às configurações do MetroCluster FC.
- Esse procedimento não causa interrupções e leva aproximadamente um dia para ser concluído (excluindo rack e pilha) quando os discos são zerados.

Antes de executar esse procedimento, a configuração do MetroCluster FC consiste em quatro nós, com um par de HA em cada local:



Na conclusão desse procedimento, a configuração do MetroCluster FC consiste em dois pares de HA em cada local:



Ambos os locais devem ser igualmente expandidos. Uma configuração MetroCluster FC não pode consistir em um número desigual de nós.

Combinações de plataforma compatíveis ao adicionar um segundo grupo de DR

As tabelas a seguir mostram as combinações de plataforma com suporte para configurações de FC MetroCluster de oito nós.

- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do ONTAP. Por exemplo, se você tiver uma configuração de oito nós, todos os oito nós devem estar executando a mesma versão do ONTAP.
- As combinações nesta tabela aplicam-se apenas a configurações de oito nós regulares ou permanentes.
- As combinações de plataforma nesta tabela **não** se aplicam se você estiver usando os procedimentos de transição ou atualização.
- Todos os nós em um grupo de DR devem ter o mesmo tipo e configuração.

Combinações de expansão de AFF e FAS MetroCluster FC compatíveis

A tabela a seguir mostra as combinações de plataforma compatíveis para expandir um sistema AFF ou FAS em uma configuração MetroCluster FC:

FAS and AFF		Eight-node DR group 2							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Eight-node DR group 1	FAS8200								
	AFF A300								
	FAS8300								
	AFF A400								
	FAS9000								
	AFF A700								
	FAS9500								
	AFF A900								

Combinações de expansão ASA MetroCluster FC compatíveis

A tabela a seguir mostra as combinações de plataforma compatíveis para expandir um sistema ASA em uma configuração MetroCluster FC:

Grupo de RD de oito nós 1	Grupo de RD de oito nós 2	Suportado?
ASA A400	ASA A400	Sim
	ASA A900	Não
ASA A900	ASA A400	Não
	ASA A900	Sim

Ativar o registo da consola

Ative o registo da consola nos seus dispositivos antes de executar esta tarefa.

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Determinando o novo layout de cabeamento

É necessário determinar o cabeamento dos novos módulos de controladora e de quaisquer novas gavetas de disco para os switches FC existentes.

Sobre esta tarefa

Esta tarefa deve ser executada em cada local do MetroCluster.

Passos

1. Use o procedimento em "Instalação e configuração do MetroCluster conectado à malha"para criar um

layout de cabeamento para o tipo de switch, usando o uso da porta para uma configuração de MetroCluster de oito nós.

O uso da porta do switch FC deve corresponder ao uso descrito no procedimento para que os arquivos de configuração de referência (RCFs) possam ser usados.

> Se o seu ambiente não puder ser habilitado de forma a que os arquivos RCF possam ser usados, você deverá configurar manualmente o sistema de acordo com as instruções encontradas em "Instalação e configuração do MetroCluster conectado à malha". Não use este procedimento se o cabeamento não puder usar arquivos RCF.

Empilhar o novo equipamento

Você precisa extrair o equipamento para os novos nós.

Passos

1. Use o procedimento no "Instalação e configuração do MetroCluster conectado à malha" para colocar em rack os novos sistemas de storage, gavetas de disco e pontes FC para SAS.

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade da configuração do MetroCluster para verificar o funcionamento correto.

Passos

1. Verifique se o MetroCluster está configurado e no modo normal em cada cluster:

   `metrocluster show`

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Verifique se o espelhamento está ativado em cada nó:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

3. Verifique se os componentes do MetroCluster estão em bom estado:

   `metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Verifique se não existem alertas de saúde:

   `system health alert show`

5. Simular uma operação de comutação:

   a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado
      `set -privilege advanced`

      Você precisa responder com **`y`** quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   b. Realize a operação de comutação com o parâmetro -simule
      `metrocluster switchover -simulate`

c. Voltar para o nível de privilégio de administrador
`set -privilege admin`

Verificando erros de configuração do MetroCluster com o Config Advisor

Você pode acessar o site de suporte da NetApp e baixar a ferramenta Config Advisor para verificar se há erros de configuração comuns.

Sobre esta tarefa

O Config Advisor é uma ferramenta de validação de configuração e verificação de integridade. Você pode implantá-lo em sites seguros e sites não seguros para coleta de dados e análise do sistema.

O suporte para Config Advisor é limitado e está disponível apenas online.

Passos

1. Vá para a página de download do Config Advisor e baixe a ferramenta.

   "NetApp Downloads: Config Advisor"

2. Execute o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Enviar uma mensagem AutoSupport personalizada antes de adicionar nós à configuração do MetroCluster

Você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Faça login no cluster em Site_A.
2. Chame uma mensagem AutoSupport indicando o início da manutenção:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   O `maintenance-window-in-hours` parâmetro especifica o comprimento da janela de manutenção e pode ser um máximo de 72 horas. Se a manutenção for concluída antes do tempo decorrido, pode emitir o seguinte comando para indicar que o período de manutenção terminou:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repita esta etapa no site do parceiro.

Recable e zone uma malha de switch para os novos nós

Desconexão do grupo de DR existente da malha

É necessário desconetar os módulos de controladora existentes dos switches FC na malha.

Sobre esta tarefa

Esta tarefa deve ser executada em cada local do MetroCluster.

Passos

1. Desative as portas HBA que conetam os módulos do controlador existentes à malha do switch que está sendo feita manutenção:

   `storage port disable -node` *`node-name`* `-port` *`port-number`*

2. Nos switches FC locais, remova os cabos das portas das pontes HBA, FC-VI e ATTO do módulo de controladora existente.

   Deve etiquetar os cabos para facilitar a identificação quando os voltar a efetuar o cabo. Somente as portas ISL devem permanecer cabeadas.

Recable e reconfigure os interrutores

Você deve aplicar os arquivos RCF para reconfigurar seu zoneamento para acomodar os novos nós.

Se você não puder usar os arquivos RCF para configurar os switches, você deverá configurar os switches manualmente. Consulte:

- "Configure os switches Brocade FC manualmente"
- "Configure os switches Cisco FC manualmente"

Passos

1. Localize os arquivos RCF para sua configuração.

   Você deve usar os arquivos RCF para uma configuração de oito nós e que corresponda ao modelo de switch.

2. Aplique os arquivos RCF, seguindo as instruções na página de download, ajustando as configurações ISL conforme necessário.
3. Certifique-se de que a configuração do interrutor é guardada.
4. Reinicie os switches FC.
5. Faça o cabeamento das pontes FC para SAS e pré-existentes, usando o layout de cabeamento criado anteriormente.

   O uso da porta do switch FC deve corresponder ao uso de oito nós do MetroCluster descrito em "Instalação e configuração do MetroCluster conectado à malha" para que os arquivos de configuração de referência (RCFs) possam ser usados.

6. Verifique se as portas estão online usando o comando correto para o switch.

Fornecedor de switch	Comando
Brocade	switchshow
Cisco	mostrar resumo da interface

7. Use o procedimento descrito no "Instalação e configuração do MetroCluster conectado à malha" para fazer o cabeamento das portas FC-VI das controladoras novas e existentes, usando o layout de cabeamento criado anteriormente.

   O uso da porta do switch FC deve corresponder ao uso de oito nós do MetroCluster descrito em "Instalação e configuração do MetroCluster conectado à malha" para que os arquivos de configuração de referência (RCFs) possam ser usados.

8. Nos nós existentes, verifique se as portas FC-VI estão online:

   ```
   metrocluster interconnect adapter show

   metrocluster interconnect mirror show
   ```

9. Faça o cabeamento das portas HBA dos controladores atual e novos.
10. Nos módulos de controladora existentes, habilite as portas conectadas à malha do switch em manutenção:

    ```
    storage port enable -node node-name -port port-ID
    ```

11. Inicie os novos controladores e inicialize-os no modo Manutenção:

    ```
    boot_ontap maint
    ```

12. Verifique se somente o armazenamento que será usado pelo novo grupo de DR está visível para os novos módulos do controlador.

    Nenhum storage usado pelo outro grupo de DR deve estar visível.

13. Volte ao início deste processo para voltar a efetuar o cabo da segunda estrutura do interrutor.

Configure o ONTAP nos novos controladores

Limpando a configuração em um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   ```
   halt
   ```

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

   ```
   set-defaults
   ```

3. Salvar o ambiente:

   `saveenv`

4. No prompt DO Loader, inicie o menu de inicialização:

   `boot_ontap menu`

5. No prompt do menu de inicialização, desmarque a configuração:

   `wipeconfig`

   Responda `yes` ao prompt de confirmação.

   O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

   Responda `yes` ao prompt de confirmação.

Atribuição de propriedade de disco em sistemas AFF

Se você estiver usando sistemas AFF em uma configuração com agregados espelhados e os nós não tiverem os discos (SSDs) corretamente atribuídos, atribua metade dos discos em cada gaveta a um nó local e a outra metade dos discos a seu nó de parceiro de HA. Você deve criar uma configuração na qual cada nó tenha o mesmo número de discos em seus pools de discos locais e remotos.

Sobre esta tarefa

Os controladores de armazenamento têm de estar no modo de manutenção.

Isso não se aplica a configurações que tenham agregados sem espelhamento, uma configuração ativo/passivo ou que tenham um número desigual de discos em pools locais e remotos.

Esta tarefa não é necessária se os discos tiverem sido corretamente atribuídos quando recebidos de fábrica.

> O pool 0 sempre contém os discos que são encontrados no mesmo local do sistema de armazenamento que os possui, enquanto o Pool 1 sempre contém os discos que são remotos para o sistema de armazenamento que os possui.

Passos

1. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.
2. Atribua os discos aos nós localizados no primeiro local (local A):

   Você deve atribuir um número igual de discos a cada pool.

   a. No primeiro nó, atribua sistematicamente metade dos discos em cada gaveta ao pool 0 e a outra metade ao pool 0 do parceiro de HA: Mais
   `disk assign -disk *disk-name* -p *pool* -n *number-of-disks*`

      Se o controlador de storage Controller_A_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você

emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Repita o processo para o segundo nó no local, atribuindo sistematicamente metade dos discos em cada gaveta ao pool 1 e a outra metade ao pool 1 do parceiro de HA
`disk assign -disk disk-name -p pool`

Se o controlador de storage Controller_A_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Atribua os discos aos nós localizados no segundo local (local B):

Você deve atribuir um número igual de discos a cada pool.

a. No primeiro nó no local remoto, atribua sistematicamente metade dos discos em cada gaveta ao pool 0 e a outra metade ao pool 0 do parceiro de HA: Mais
`disk assign -disk disk-name -p pool`

Se o controlador de storage Controller_B_1 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. Repita o processo para o segundo nó no local remoto, atribuindo sistematicamente metade dos discos em cada gaveta ao pool 1 e a outra metade ao pool 1 do parceiro de HA:

`disk assign -disk disk-name -p pool`

Se o controlador de storage Controller_B_2 tiver quatro gavetas, cada uma com SSDs de 8 TB, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirme as atribuições de disco:

   `storage show disk`

5. Sair do modo de manutenção:

   `halt`

6. Apresentar o menu de arranque:

   `boot_ontap menu`

7. Em cada nó, selecione a opção **4** para inicializar todos os discos.

Atribuição de propriedade de disco em sistemas que não sejam AFF

Se os nós do MetroCluster não tiverem os discos corretamente atribuídos ou se você estiver usando DS460C compartimentos de disco na sua configuração, será necessário atribuir discos a cada um dos nós na configuração do MetroCluster de acordo com compartimento a compartimento. Você criará uma configuração na qual cada nó tem o mesmo número de discos em seus pools de discos locais e remotos.

Sobre esta tarefa

Os controladores de armazenamento têm de estar no modo de manutenção.

Se a configuração não incluir DS460C compartimentos de disco, essa tarefa não será necessária se os discos tiverem sido atribuídos corretamente quando recebidos de fábrica.

> O pool 0 sempre contém os discos que são encontrados no mesmo local do sistema de armazenamento que os possui.
>
> O pool 1 sempre contém os discos que são remotos para o sistema de storage que os possui.

Se a configuração incluir DS460C compartimentos de disco, você deve atribuir manualmente os discos usando as seguintes diretrizes para cada gaveta de 12 discos:

Atribuir estes discos na gaveta…	Para este nó e pool…
0 - 2	Pool do nó local 0
3 - 5	Pool do nó de PARCEIRO HA 0

6 - 8	Parceiro de DR do pool de nós locais 1
9 - 11	Parceiro de DR do pool de parceiros de HA 1

Esse padrão de atribuição de disco garante que um agregado seja minimamente afetado caso uma gaveta fique offline.

Passos

1. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.
2. Atribua os compartimentos de disco aos nós localizados no primeiro local (local A):

   Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1.

   Você deve atribuir um número igual de prateleiras a cada pool.

   a. No primeiro nó, atribua sistematicamente as gavetas de disco locais ao pool 0 e às gavetas de disco remotas ao pool 1:

      `disk assign -shelf local-switch-name:shelf-name.port -p pool`

      Se o controlador de storage Controller_A_1 tiver quatro compartimentos, você emitirá os seguintes comandos:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
      ```

   b. Repita o processo para o segundo nó no local, atribuindo sistematicamente as gavetas de disco locais ao pool 0 e as gavetas de disco remotas ao pool 1:

      `disk assign -shelf local-switch-name:shelf-name.port -p pool`

      Se o controlador de storage Controller_A_2 tiver quatro compartimentos, você emitirá os seguintes comandos:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
      *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

      *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
      *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
      ```

3. Atribua os compartimentos de disco aos nós localizados no segundo local (local B):

   Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de

disco localizados no local do parceiro são atribuídos ao pool 1.

Você deve atribuir um número igual de prateleiras a cada pool.

a. No primeiro nó no local remoto, atribua sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1:

   `disk assign -shelf local-switch-nameshelf-name -p pool`

   Se o controlador de storage Controller_B_1 tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. Repita o processo para o segundo nó no local remoto, atribuindo sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1:

   `disk assign -shelf shelf-name -p pool`

   Se o controlador de storage Controller_B_2 tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirme as atribuições do compartimento:

   `storage show shelf`

5. Sair do modo de manutenção:

   `halt`

6. Apresentar o menu de arranque:

   `boot_ontap menu`

7. Em cada nó, selecione a opção **4** para inicializar todos os discos.

Verificando o estado ha-config dos componentes

Em uma configuração MetroCluster, o estado ha-config do módulo do controlador e dos

componentes do chassi deve ser definido como **mcc** para que eles iniciem corretamente.

Sobre esta tarefa

- O sistema tem de estar no modo de manutenção.
- Esta tarefa deve ser executada em cada novo módulo do controlador.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado de HA para todos os componentes deve ser "mcc".

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA para o módulo do controlador:

   `ha-config modify controller mcc`

3. Se o estado do sistema apresentado do chassis não estiver correto, defina o estado HA para o chassis:

   `ha-config modify chassis mcc`

4. Repita estas etapas no outro nó de substituição.

Inicializando os novos controladores e juntando-os ao cluster

Para unir os novos controladores ao cluster, você deve inicializar cada novo módulo de controladora e usar o assistente de configuração do cluster do ONTAP para identificar o cluster que será associado.

Antes de começar

Você deve ter cabeado a configuração do MetroCluster.

Você não deve ter configurado o processador de serviço antes de executar esta tarefa.

Sobre esta tarefa

Essa tarefa deve ser executada em cada uma das novas controladoras em ambos os clusters na configuração MetroCluster.

Passos

1. Se você ainda não fez isso, ligue cada nó e deixe-os inicializar completamente.

   Se o sistema estiver no modo Manutenção, emita o `halt` comando para sair do modo Manutenção e, em seguida, emita o seguinte comando a partir do prompt Loader:

   `boot_ontap`

   O módulo do controlador entra no assistente de configuração do nó.

   A saída deve ser semelhante ao seguinte:

```
Welcome to node setup

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
                Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. Ative a ferramenta AutoSupport seguindo as instruções fornecidas pelo sistema.
3. Responda aos prompts para configurar a interface de gerenciamento de nós.

   Os prompts são semelhantes aos seguintes:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Confirme se os nós estão configurados no modo de alta disponibilidade:

   `storage failover show -fields mode`

   Caso contrário, você deve emitir o seguinte comando em cada nó e, em seguida, reinicializar o nó:

   `storage failover modify -mode ha -node localhost`

   Este comando configura o modo de alta disponibilidade, mas não ativa o failover de armazenamento. O failover de armazenamento é ativado automaticamente quando você emite o `metrocluster configure` comando mais tarde no processo de configuração.

5. Confirme se você tem quatro portas configuradas como interconexões de cluster:

   `network port show`

   O exemplo a seguir mostra a saída para dois controladores em cluster_A. Se for uma configuração de MetroCluster de dois nós, a saída mostrará apenas um nó.

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Como você está usando a CLI para configurar o cluster, saia do assistente de configuração do nó:

   `exit`

7. Inicie sessão na conta de administrador utilizando o `admin` nome de utilizador.
8. Inicie o assistente Configuração de cluster e, em seguida, junte-se ao cluster existente:

   `cluster setup`

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


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

9. Depois de concluir o assistente **Cluster Setup** e ele sair, verifique se o cluster está ativo e se o nó está em bom estado:

   `cluster show`

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

```
cluster_A::> cluster show
Node                 Health  Eligibility
-------------------- ------- ------------
node_A_1             true    true
node_A_2             true    true
node_A_3             true    true
```

   Se for necessário alterar qualquer uma das configurações inseridas para o SVM ou nó SVM admin, você poderá acessar o assistente **Configuração de cluster** usando o `cluster setup command`.

Configure os clusters em uma configuração do MetroCluster

Configurar LIFs entre clusters

Saiba como configurar LIFs entre clusters em portas dedicadas e compartilhadas.

Configurar LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas para aumentar a largura de banda disponível para tráfego de replicação.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que as portas "e0e" e "e0f" não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

   `network interface failover-groups create -vserver <system_SVM> -failover -group <failover_group> -targets <physical_or_logical_ports>`

   O exemplo a seguir atribui as portas "e0e" e "e0f" ao grupo de failover "intercluster01" no SVM do sistema "cluster01":

```
cluster01::> network interface failover-groups create -vserver
cluster01 -failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

   `network interface failover-groups show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-
01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-
01:e0d,
                                  cluster01-02:e0c, cluster01-
02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Versão de ONTAP	Comando
9,6 e mais tarde	`network interface create -vserver <system_SVM> -lif <LIF_name> -service-policy default-intercluster -home -node <node> -home-port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`
9,5 e anteriores	`network interface create -vserver system_SVM -lif <LIF_name> -role intercluster -home-node <node> -home -port <port> -address <port_IP> -netmask <netmask> -failover-group <failover_group>`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" no grupo de failover "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

Em ONTAP 9.6 e posteriores:
`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:
`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. Verifique se as LIFs entre clusters são redundantes:

Em ONTAP 9.6 e posteriores:

```
network interface show -service-policy default-intercluster -failover
```

Em ONTAP 9.5 e anteriores:

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta SVM "e0e" falharão para a porta "e0f".

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados para reduzir o número de portas necessárias para a rede entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
```

2. Criar LIFs entre clusters no sistema:

Em ONTAP 9.6 e posteriores:
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
Em ONTAP 9.5 e anteriores:
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

Em ONTAP 9.6 e posteriores:
`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:
`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. Verifique se as LIFs entre clusters são redundantes:

Em ONTAP 9.6 e posteriores:

`network interface show –service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:
`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "e0c" falharão para a porta "e0d".

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Espelhamento dos agregados de raiz

É necessário espelhar os agregados raiz para fornecer proteção de dados.

Por padrão, o agregado raiz é criado como agregado do tipo RAID-DP. Você pode alterar o agregado raiz de RAID-DP para o agregado do tipo RAID4. O comando a seguir modifica o agregado raiz para o agregado do tipo RAID4:

```
storage aggregate modify –aggregate aggr_name -raidtype raid4
```

Em sistemas que não sejam ADP, o tipo RAID do agregado pode ser modificado do RAID-DP padrão para RAID4 antes ou depois que o agregado é espelhado.

Passos

1. Espelhar o agregado raiz:

`storage aggregate mirror aggr_name`

O comando a seguir espelha o agregado raiz para controller_A_1:

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

Isso reflete o agregado, por isso consiste em um Plex local e um Plex remoto localizado no local remoto de MetroCluster.

2. Repita a etapa anterior para cada nó na configuração do MetroCluster.

Implementando a configuração do MetroCluster

Você deve executar o `metrocluster configure -refresh true` comando para iniciar a proteção de dados nos nós adicionados a uma configuração do MetroCluster.

Sobre esta tarefa

Você emite o `metrocluster configure -refresh true` comando uma vez, em um dos nós recém-adicionados, para atualizar a configuração do MetroCluster. Não é necessário emitir o comando em cada um dos sites ou nós.

```
`metrocluster configure -refresh true`O comando emparelhará automaticamente os dois nós com as IDs de sistema mais baixas em cada um dos dois clusters como parceiros de recuperação de desastres (DR). Em uma configuração de MetroCluster de quatro nós, há dois pares de parceiros de DR. O segundo par de DR é criado a partir dos dois nós com IDs de sistema mais altas.
```

Passos

1. Atualize a configuração do MetroCluster:

   a. Entrar no modo de privilégio avançado:

      `set -privilege advanced`

   b. Atualize a configuração do MetroCluster em um dos novos nós `metrocluster configure -refresh true`

      O exemplo a seguir mostra a configuração do MetroCluster atualizada em ambos os grupos de DR:

```
controller_A_2::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

+

```
controller_A_4::*> metrocluster configure -refresh true

[Job 740] Job succeeded: Configure is successful.
```

a. Voltar ao modo de privilégios de administrador:

```
set -privilege admin
```

2. Verifique o status da rede no local A:

```
network port show
```

O exemplo a seguir mostra o uso da porta de rede em uma configuração MetroCluster de quatro nós:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster:

a. Verifique a configuração do local A:

```
metrocluster show
```

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

a. Verifique a configuração a partir do local B
`metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

Sobre esta tarefa

- Você deve saber quais unidades serão usadas no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.
- As unidades são de propriedade de um nó específico; quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.

  Em sistemas que usam ADP, agregados são criados usando partições nas quais cada unidade é particionada em partições P1, P2 e P3.

- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.

  "Gerenciamento de disco e agregado"

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

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

   `storage disk show -spare -owner` *`node_name`*

2. Criar o agregado:

   `storage aggregate create -mirror true`

   Se você estiver conetado ao cluster na interface de gerenciamento de cluster, poderá criar um agregado em qualquer nó do cluster. Para garantir que o agregado seja criado em um nó específico, use o `-node` parâmetro ou especifique as unidades que são de propriedade desse nó.

   Você pode especificar as seguintes opções:

   - Nó inicial do agregado (ou seja, o nó que possui o agregado em operação normal)
   - Lista de unidades específicas que devem ser adicionadas ao agregado
   - Número de unidades a incluir

     Na configuração mínima suportada, na qual um número limitado de unidades está disponível, você deve usar a opção force-small-Aggregate para permitir a criação de um agregado RAID-DP de três discos.

   - Estilo de checksum para usar para o agregado
   - Tipo de unidades a utilizar
   - Tamanho das unidades a utilizar
   - Velocidade de condução a utilizar
   - Tipo RAID para grupos RAID no agregado
   - Número máximo de unidades que podem ser incluídas em um grupo RAID
   - Se unidades com RPM diferentes são permitidas

     Para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

     O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Configuração de pontes FC para SAS para monitoramento de integridade

Saiba como configurar as pontes FC-para-SAS para monitoramento de integridade.

Sobre esta tarefa

- Ferramentas de monitoramento SNMP de terceiros não são suportadas para bridges FibreBridge.
- A partir do ONTAP 9.8, as bridges FC para SAS são monitoradas por meio de conexões na banda por padrão, e não é necessária configuração adicional.

> A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passo

1. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:

   a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
9,5 e mais tarde	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9,4 e anteriores	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   b. Verifique se a ponte foi adicionada e está configurada corretamente:

      `storage bridge show`

      Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de integridade do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

      O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model               Bridge WWN
------------------  ------------ ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Movimentação de um volume de metadados nas configurações do MetroCluster

Você pode mover um volume de metadados de um agregado para outro agregado em uma configuração do MetroCluster. Talvez você queira mover um volume de metadados quando o agregado de origem for desativado ou sem espelhamento, ou por outros motivos que tornam o agregado inelegível.

Sobre esta tarefa

- Você deve ter o administrador de cluster Privileges para executar esta tarefa.
- O agregado de destino deve ser espelhado e não deve estar no estado degradado.
- O espaço disponível no agregado de destino deve ser maior que o volume de metadados que você está movendo.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Identifique o volume de metadados que deve ser movido:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW             -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW             -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identificar um agregado-alvo qualificado:

   `metrocluster check config-replication show-aggregate-eligibility`

   O comando a seguir identifica os agregados em cluster_A que estão qualificados para hospedar volumes de metadados:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

No exemplo anterior, Node_A_1_aggr2 e Node_A_2_aggr2 são elegíveis.

4. Iniciar a operação de movimentação de volume:

   `volume move start -vserver` *`svm_name`* `-volume` *`metadata_volume_name`* `-destination -aggregate` *`destination_aggregate_name`*`*`

   O seguinte comando move o volume de metadados "MDV_CRS_14c00d4ac9f311e7922800a0984395f1" de "Aggregate Node_A_1_aggr1" para "Aggregate Node_A_1_aggr2":

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verifique o estado da operação de movimentação de volume:

```
volume move show -volume vol_constituent_name
```

6. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente. Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster. Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Sobre esta tarefa

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Os comandos subsequentes `metrocluster check show` não mostram a saída esperada.

Passos

1. Verificar a configuração:

```
metrocluster check run
```

O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Exibir resultados mais detalhados do comando mais recente `metrocluster check run`:

   ```
   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

   Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

   O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                 Check
Result
---------------       --------------------      ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
```

```
ok
                    controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2      controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                    controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok

18 entries were displayed.
```

O exemplo a seguir mostra a `metrocluster check cluster show` saída do comando para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

```
Last Checked On: 9/13/2017 20:47:04

Cluster               Check                             Result
--------------------- --------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready       not-applicable
                      switchback-ready                  not-applicable
                      job-schedules                     ok
                      licenses                          ok
                      periodic-check-enabled            ok
mccint-fas9000-0304
                      negotiated-switchover-ready       not-applicable
                      switchback-ready                  not-applicable
                      job-schedules                     ok
                      licenses                          ok
                      periodic-check-enabled            ok
10 entries were displayed.
```

Verificando erros de configuração do MetroCluster com o Config Advisor

Você pode acessar o site de suporte da NetApp e baixar a ferramenta Config Advisor para verificar se há erros de configuração comuns.

Sobre esta tarefa

O Config Advisor é uma ferramenta de validação de configuração e verificação de integridade. Você pode implantá-lo em sites seguros e sites não seguros para coleta de dados e análise do sistema.

O suporte para Config Advisor é limitado e está disponível apenas online.

Passos

1. Vá para a página de download do Config Advisor e baixe a ferramenta.

   "NetApp Downloads: Config Advisor"

2. Execute o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Enviando uma mensagem AutoSupport personalizada depois de adicionar nós à configuração do MetroCluster

Você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está concluída.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Faça login no cluster em Site_A.
2. Chamar uma mensagem AutoSupport indicando o fim da manutenção:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Repita esta etapa no site do parceiro.

Verificando switchover, cura e switchback

Você deve verificar as operações de switchover, recuperação e switchback da configuração do MetroCluster.

Passos

1. Use os procedimentos para comutação negociada, recuperação e switchback no "Gerenciamento de MetroCluster e recuperação de desastres".

Expanda uma configuração IP do MetroCluster

Dependendo da versão do ONTAP, você pode expandir sua configuração IP do MetroCluster adicionando quatro novos nós como um novo grupo de DR.

A partir do ONTAP 9.13,1, é possível expandir temporariamente uma configuração MetroCluster de oito nós para atualizar os controladores e o armazenamento. Consulte "Atualizando uma configuração de IP MetroCluster de quatro ou oito nós (ONTAP 9.8 e posterior)" para obter mais informações.

A partir do ONTAP 9.9,1, é possível adicionar quatro novos nós à configuração IP do MetroCluster como um segundo grupo de DR. Isso cria uma configuração MetroCluster de oito nós.

Antes de começar

- Os nós antigos e novos devem estar executando a mesma versão do ONTAP.
- Este procedimento descreve as etapas necessárias para adicionar um grupo de DR de quatro nós a uma configuração IP do MetroCluster existente. Se você estiver atualizando uma configuração de oito nós, repita todo o procedimento para cada grupo de DR, adicionando um de cada vez.
- Verifique se os modelos de plataforma antigos e novos são suportados para mistura de plataforma.

  "NetApp Hardware Universe"

- Verifique se os modelos de plataforma antigos e novos são suportados pelos switches IP.

  "NetApp Hardware Universe"

- Se você estiver "Atualizando uma configuração de IP MetroCluster de quatro ou oito nós", os novos nós precisam ter storage suficiente para acomodar os dados dos nós antigos, juntamente com discos adequados para agregados de raiz e discos sobressalentes.
- Verifique se você tem um domínio de broadcast padrão criado nos nós antigos.

  Quando você adiciona novos nós a um cluster existente sem um domínio de broadcast padrão, as LIFs de gerenciamento de nós são criadas para os novos nós usando identificadores únicos universais (UUIDs) em vez dos nomes esperados. Para obter mais informações, consulte o artigo da base de dados de Conhecimento "LIFs de gerenciamento de nós em nós recém-adicionados gerados com nomes UUID" .

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Exemplo de nomeação neste procedimento

Este procedimento usa nomes de exemplo em todo o para identificar os grupos de DR, nós e switches envolvidos.

Grupos DR	Cluster_A no site_A	Cluster_B no local_B
dr_group_1-old	• Node_A_1-old • Node_A_2-old	• Node_B_1-old • Node_B_2-old
dr_group_2-novo	• Node_A_3-novo • Node_A_4-novo	• Node_B_3-novo • Node_B_4-novo

Combinações de plataforma compatíveis ao adicionar um segundo grupo de DR

As tabelas a seguir mostram as combinações de plataforma suportadas para configurações IP MetroCluster de oito nós.

- Todos os nós na configuração do MetroCluster devem estar executando a mesma versão do ONTAP. Por exemplo, se você tiver uma configuração de oito nós, todos os oito nós devem estar executando a mesma versão do ONTAP.
- As combinações nesta tabela aplicam-se apenas a configurações de nós 8 regulares ou permanentes.
- As combinações de plataforma mostradas nesta tabela **não** se aplicam se você estiver usando os procedimentos de transição ou atualização.
- Todos os nós em um grupo de DR devem ter o mesmo tipo e configuração.

Combinações de expansão IP AFF e FAS MetroCluster suportadas

A tabela a seguir mostra as combinações de plataforma compatíveis para expandir um sistema AFF ou FAS em uma configuração IP MetroCluster:

FAS and AFF		Eight-node DR group 2												
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF A90	AFF A1K
Eight-node DR group 1	AFF A150	Note 2												
	FAS2750 AFF A220													
	FAS500f AFF C250 AFF A250													
	FAS8200 AFF A300				Note 1									
	AFF A320					Note 1								
	FAS8300 AFF C400 AFF A400													
	FAS8700													
	FAS9000 AFF A700								Note 1					
	AFF A70													
	AFF C800 AFF A800													
	FAS9500 AFF A900													
	AFF A90													
	AFF A1K													

- **Nota 1**: ONTAP 9.9,1 ou posterior (ou a versão mínima do ONTAP suportada na plataforma) é necessária para estas combinações.
- **Nota 2**: ONTAP 9.13,1 ou posterior (ou a versão mínima do ONTAP suportada na plataforma) é necessária para estas combinações.

Combinações de expansão IP ASA MetroCluster suportadas

A tabela a seguir mostra as combinações de plataforma suportadas para expandir um sistema ASA em uma configuração IP do MetroCluster:

ASA		Eight-node DR group 2							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Eight-node DR group 1	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

Enviar uma mensagem AutoSupport personalizada antes da manutenção

Antes de executar a manutenção, você deve emitir uma mensagem AutoSupport para notificar o suporte técnico da NetApp de que a manutenção está em andamento. Informar o suporte técnico de que a manutenção está em andamento impede que ele abra um caso partindo do pressuposto de que ocorreu uma interrupção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada site do MetroCluster.

Passos

1. Para impedir a geração automática de casos de suporte, envie uma mensagem AutoSupport para indicar que a atualização está em andamento.

   a. Emita o seguinte comando:

   ```
   system node autosupport invoke -node * -type all -message "MAINT=10h
   ```

```
Upgrading <old-model> to <new-model>
```

Este exemplo especifica uma janela de manutenção de 10 horas. Você pode querer permitir tempo adicional, dependendo do seu plano.

Se a manutenção for concluída antes do tempo decorrido, você poderá invocar uma mensagem AutoSupport indicando o fim do período de manutenção:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Repita o comando no cluster de parceiros.

Considerações para VLANs ao adicionar um novo grupo de DR

- As considerações de VLAN a seguir se aplicam ao expandir uma configuração de IP MetroCluster:

  Certas plataformas usam uma VLAN para a interface IP do MetroCluster. Por padrão, cada uma das duas portas usa uma VLAN diferente: 10 e 20.

  Se suportado, você também pode especificar uma VLAN diferente (não padrão) maior que 100 (entre 101 e 4095) usando o `-vlan-id` parâmetro no `metrocluster configuration-settings interface create` comando.

  As seguintes plataformas **não** suportam o `-vlan-id` parâmetro:

  - FAS8200 e AFF A300
  - AFF A320
  - FAS9000 e AFF A700
  - AFF C800, ASA C800, AFF A800 e ASA A800

    Todas as outras plataformas suportam o `-vlan-id` parâmetro.

    As atribuições de VLAN padrão e válidas dependem se a plataforma suporta o `-vlan-id` parâmetro:

Plataformas que suportam <code>-vlan-id</code>

VLAN predefinida:

- Quando o `-vlan-id` parâmetro não é especificado, as interfaces são criadas com VLAN 10 para as portas "A" e VLAN 20 para as portas "B".
- A VLAN especificada deve corresponder à VLAN selecionada no RCF.

Intervalos de VLAN válidos:

- VLAN 10 e 20 padrão
- VLANs 101 e superior (entre 101 e 4095)

Plataformas que não suportam <code>-vlan-id</code>

VLAN predefinida:

- Não aplicável. A interface não requer que uma VLAN seja especificada na interface MetroCluster. A porta do switch define a VLAN que é usada.

Intervalos de VLAN válidos:

- Todas as VLANs não explicitamente excluídas ao gerar o RCF. O RCF alerta-o se a VLAN for inválida.

- Ambos os grupos de DR usam as mesmas VLANs quando você expande de uma configuração de MetroCluster de quatro nós para oito nós.
- Se ambos os grupos de DR não puderem ser configurados usando a mesma VLAN, você deverá atualizar o grupo de DR que não suporta o `vlan-id` parâmetro para usar uma VLAN suportada pelo outro grupo de DR.
- Dependendo da versão do ONTAP, você pode alterar algumas propriedades da interface IP do MetroCluster após a configuração inicial. "Modifique as propriedades de uma interface IP do MetroCluster"Consulte para obter detalhes sobre o que é suportado.

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade e a conectividade da configuração do MetroCluster antes de executar a expansão.

Passos

1. Verifique a operação da configuração do MetroCluster no ONTAP:
   a. Verifique se o sistema é multipathed:

      ```
      node run -node <node-name> sysconfig -a
      ```

   b. Verifique se há alertas de integridade em ambos os clusters:

      ```
      system health alert show
      ```

   c. Confirme a configuração do MetroCluster e se o modo operacional está normal:

      ```
      metrocluster show
      ```

d. Execute uma verificação MetroCluster:

```
metrocluster check run
```

e. Apresentar os resultados da verificação MetroCluster:

```
metrocluster check show
```

f. Execute o Config Advisor.

"NetApp Downloads: Config Advisor"

g. Depois de executar o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

2. Verifique se o cluster está em bom estado:

```
cluster show
```

```
cluster_A::> cluster show
Node            Health  Eligibility
--------------- ------  -----------
node_A_1        true    true
node_A_2        true    true

cluster_A::>
```

3. Verifique se todas as portas do cluster estão ativas:

```
network port show -ipspace Cluster
```

```
cluster_A::> network port show -ipspace Cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show -vserver Cluster`

   Cada LIF de cluster deve exibir True para is Home e ter um Administrador de Status/Oper de up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

   `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Removendo a configuração dos aplicativos de monitoramento

Se a configuração existente for monitorada com o software tiebreaker do MetroCluster, o Mediador do ONTAP ou outros aplicativos de terceiros (por exemplo, o ClusterLion) que possam iniciar um switchover, você deverá remover a configuração do MetroCluster do software de monitoramento antes da atualização.

Passos

1. Remova a configuração do MetroCluster existente do tiebreaker, Mediator ou outro software que possa iniciar o switchover.

Se você estiver usando…	Use este procedimento…
Desempate	"Remoção das configurações do MetroCluster".
Mediador	Execute o seguinte comando no prompt do ONTAP: `metrocluster configuration-settings mediator remove`
Aplicativos de terceiros	Consulte a documentação do produto.

2. Remova a configuração do MetroCluster existente de qualquer aplicativo de terceiros que possa iniciar o switchover.

   Consulte a documentação da aplicação.

Preparar os novos módulos do controlador

Você deve preparar os quatro novos nós do MetroCluster e instalar a versão correta do ONTAP.

Sobre esta tarefa

Esta tarefa deve ser executada em cada um dos novos nós:

- Node_A_3-novo
- Node_A_4-novo
- Node_B_3-novo
- Node_B_4-novo

Nestas etapas, você limpa a configuração nos nós e limpa a região da caixa de correio em novas unidades.

Passos

1. Colocar em rack os novos controladores.
2. Faça o cabeamento dos novos nós IP do MetroCluster aos switches IP, conforme mostrado na "Cable os switches IP".
3. Configure os nós IP do MetroCluster usando os seguintes procedimentos:
   a. "Reúna as informações necessárias"
   b. "Restaure os padrões do sistema em um módulo do controlador"
   c. "Verifique o estado ha-config dos componentes"
   d. "Atribuir manualmente unidades para o pool 0 (ONTAP 9.4 e posterior)"
4. No modo Manutenção, emita o comando halt para sair do modo Manutenção e, em seguida, emita o comando boot_ONTAP para inicializar o sistema e chegar à configuração do cluster.

   Não conclua o assistente de cluster ou o assistente de nó neste momento.

Atualize arquivos RCF

Se você estiver instalando o novo firmware do switch, você deve instalar o firmware do switch antes de atualizar o arquivo RCF.

Sobre esta tarefa

Este procedimento interrompe o tráfego no switch onde o arquivo RCF é atualizado. O tráfego será retomado quando o novo arquivo RCF for aplicado.

Passos

1. Verifique a integridade da configuração.

   a. Verifique se os componentes do MetroCluster estão em bom estado:

      `metrocluster check run`

      ```
      cluster_A::*> metrocluster check run
      ```

      A operação é executada em segundo plano.

b. Após a `metrocluster check run` conclusão da operação, execute `metrocluster check show` para visualizar os resultados.

   Após cerca de cinco minutos, são apresentados os seguintes resultados:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Verificar o estado do funcionamento da verificação do MetroCluster em curso:

   `metrocluster operation history show -job-id 38`

b. Verifique se não há alertas de saúde:

   `system health alert show`

2. Preparar os comutadores IP para a aplicação dos novos ficheiros RCF.

   Siga as etapas para o fornecedor do switch:

   - "Redefina o switch IP Broadcom para os padrões de fábrica"
   - "Redefina o switch IP Cisco para os padrões de fábrica"
   - "Redefina o switch NVIDIA IP SN2100 para os padrões de fábrica"

3. Baixe e instale o arquivo RCF IP, dependendo do fornecedor do switch.

   Atualize os interrutores pela seguinte ordem: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

   - "Baixe e instale os arquivos Broadcom IP RCF"
   - "Transfira e instale os ficheiros Cisco IP RCF"
   - "Transfira e instale os ficheiros NVIDIA IP RCF"

Se você tiver uma configuração de rede L2 compartilhada ou L3, talvez seja necessário ajustar as portas ISL nos switches intermediários/clientes. O modo de porta do switch pode mudar de modo 'Access' para 'trunk'. Apenas prossiga para atualizar o segundo par de switches (A_2, B_2) se a conetividade de rede entre os switches A_1 e B_1 estiver totalmente operacional e a rede estiver em bom estado.

Junte os novos nós aos clusters

Você deve adicionar os quatro novos nós IP do MetroCluster à configuração existente do MetroCluster.

Sobre esta tarefa

Você deve executar essa tarefa em ambos os clusters.

Passos

1. Adicione os novos nós IP do MetroCluster à configuração do MetroCluster existente.
   a. Junte o primeiro novo nó IP do MetroCluster (node_A_1-novo) à configuração IP do MetroCluster existente.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: 172.17.8.93

172.17.8.93 is not a valid port.
```

```
The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


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


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Junte o segundo novo nó IP do MetroCluster (node_A_2-novo) à configuração IP do MetroCluster existente.

2. Repita estas etapas para unir node_B_1-novo e node_B_2-novo ao cluster_B.

Configurando LIFs entre clusters, criando interfaces MetroCluster e espelhando agregados de raiz

Você deve criar LIFs de peering de cluster, criar as interfaces MetroCluster nos novos nós IP do MetroCluster.

Sobre esta tarefa

- A porta inicial usada nos exemplos é específica da plataforma. Você deve usar a porta inicial específica para sua plataforma de nó IP do MetroCluster.
- Reveja as informações em Considerações para VLANs ao adicionar um novo grupo de DR antes de executar esta tarefa.

Passos

1. Nos novos nós IP do MetroCluster, configure as LIFs entre clusters usando os seguintes procedimentos:

   "Configurando LIFs entre clusters em portas dedicadas"

   "Configurando LIFs entre clusters em portas de dados compartilhados"

2. Em cada site, verifique se o peering de cluster está configurado:

   ```
   cluster peer show
   ```

   O exemplo a seguir mostra a configuração de peering de cluster no cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   O exemplo a seguir mostra a configuração de peering de cluster no cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. Crie o grupo de DR para os nós IP do MetroCluster:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   Para obter mais informações sobre as configurações e conexões do MetroCluster, consulte o seguinte:

   "Considerações para configurações IP do MetroCluster"

"Criando o grupo DR"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verifique se o grupo de DR foi criado.

`metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                       node_A_1-old        node_B_1-old
                                       node_A_2-old        node_B_2-old
            cluster_B
                                       node_B_1-old        node_A_1-old
                                       node_B_2-old        node_A_2-old
2           cluster_A
                                       node_A_1-new        node_B_1-new
                                       node_A_2-new        node_B_2-new
            cluster_B
                                       node_B_1-new        node_A_1-new
                                       node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Configure as interfaces IP do MetroCluster para os nós IP do MetroCluster recém-ingressados:

- Se suportado, você pode especificar uma VLAN diferente (não padrão) maior que 100 (entre 101 e 4095) usando o `-vlan-id` parâmetro no `metrocluster configuration-settings interface create` comando. Considerações para VLANs ao adicionar um novo grupo de DRConsulte para obter informações sobre a plataforma suportada.
- Você pode configurar as interfaces IP do MetroCluster a partir de qualquer cluster.

`metrocluster configuration-settings interface create -cluster-name`

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verifique se as interfaces IP do MetroCluster são criadas:

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                Home Port: e1a
                     172.17.28.11    255.255.255.0   -
completed
                Home Port: e1b
                     172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                Home Port: e1a
                     172.17.28.13    255.255.255.0   -
completed
                Home Port: e1b
                     172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                Home Port: e1a
                     172.17.28.12    255.255.255.0   -
completed
                Home Port: e1b
                     172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Conete as interfaces IP do MetroCluster:

   `metrocluster configuration-settings connection connect`

   Esse comando pode levar vários minutos para ser concluído.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verifique se as conexões estão corretamente estabelecidas: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
            node_B_1-new
                Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Verifique a atribuição automática e o particionamento do disco:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Espelhar os agregados de raiz:

`storage aggregate mirror -aggregate aggr0_node_A_1-new`

Você deve concluir esta etapa em cada nó IP do MetroCluster.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                  Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verifique se os agregados raiz estão espelhados:

`storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Finalizando a adição dos novos nós

Você precisa incorporar o novo grupo de DR à configuração do MetroCluster e criar agregados de dados espelhados nos novos nós.

Passos

1. Atualize a configuração do MetroCluster:

   a. Entrar no modo de privilégio avançado:

      ```
      set -privilege advanced
      ```

   b. Atualize a configuração do MetroCluster em qualquer um dos nós:

Se a sua configuração do MetroCluster tiver…	Então faça isso…
Vários agregados de dados	A partir do prompt de qualquer nó, execute: `metrocluster configure <node-name>`
Um único agregado de dados espelhados em um ou ambos os locais	A partir do prompt de qualquer nó, configure o MetroCluster com o `-allow-with-one-aggregate true` parâmetro: `metrocluster configure -allow-with-one-aggregate true <node-name>`

c. Reinicie cada um dos novos nós:

```
node reboot -node <node_name> -inhibit-takeover true
```

Você não precisa reiniciar os nós em uma ordem específica, mas você deve esperar até que um nó seja totalmente inicializado e todas as conexões sejam estabelecidas antes de reiniciar o próximo nó.

a. Voltar ao modo de privilégios de administrador:

```
set -privilege admin
```

2. Crie agregados de dados espelhados em cada um dos novos nós MetroCluster:

```
storage aggregate create -aggregate <aggregate-name> -node <node-name>
-diskcount <no-of-disks> -mirror true
```

Você deve criar pelo menos um agregado de dados espelhados por local. Recomenda-se ter dois agregados de dados espelhados por local em nós IP do MetroCluster para hospedar os volumes MDV. No entanto, um único agregado por local é suportado (mas não recomendado). É aceitável que um site do MetroCluster tenha um único agregado de dados espelhados e o outro site tenha mais de um agregado de dados espelhados.

O exemplo a seguir mostra a criação de um agregado em node_A_1-novo.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
```

```
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. Verifique se os nós são adicionados ao grupo de DR.

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Mova os volumes MDV_CRS no modo de privilégio avançado.

   a. Apresentar os volumes para identificar os volumes MDV:

      Se você tiver um único agregado de dados espelhados por local, mova ambos os volumes MDV para esse único agregado. Se você tiver dois ou mais agregados de dados espelhados, mova cada volume MDV para um agregado diferente.

      Se você estiver expandindo uma configuração MetroCluster de quatro nós para uma configuração permanente de oito nós, mova um dos volumes MDV para o novo grupo de DR.

      O exemplo a seguir mostra os volumes MDV na `volume show` saída:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Defina o nível de privilégio avançado:

```
set -privilege advanced
```

c. Mova os volumes MDV, um de cada vez:

```
volume move start -volume <mdv-volume> -destination-aggregate <aggr-on-new-
node> -vserver <svm-name>
```

O exemplo a seguir mostra o comando e a saída para mover "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" para agregar "data_A3" em "node_A_3".

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Use o comando volume show para verificar se o volume MDV foi movido com sucesso:

```
volume show <mdv-name>
```

A saída seguinte mostra que o volume MDV foi movido com sucesso.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

5. Mova o epsilon de um nó antigo para um novo nó:

a. Identificar qual nó tem atualmente o epsilon:

```
cluster show -fields epsilon
```

```
cluster_B::*> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Defina epsilon como false no nó antigo (node_A_1-old):

```
cluster modify -node <old-node> -epsilon false*
```

c. Defina epsilon como true no novo nó (node_A_3-novo):

```
cluster modify -node <new-node> -epsilon true
```

d. Verifique se o epsilon foi movido para o nó correto:

```
cluster show -fields epsilon
```

```
cluster_A::*> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

6. Se o sistema oferecer suporte a criptografia completa, você poderá "Ative a criptografia de ponta a ponta" no novo grupo de DR.

Removendo um grupo de recuperação de desastres

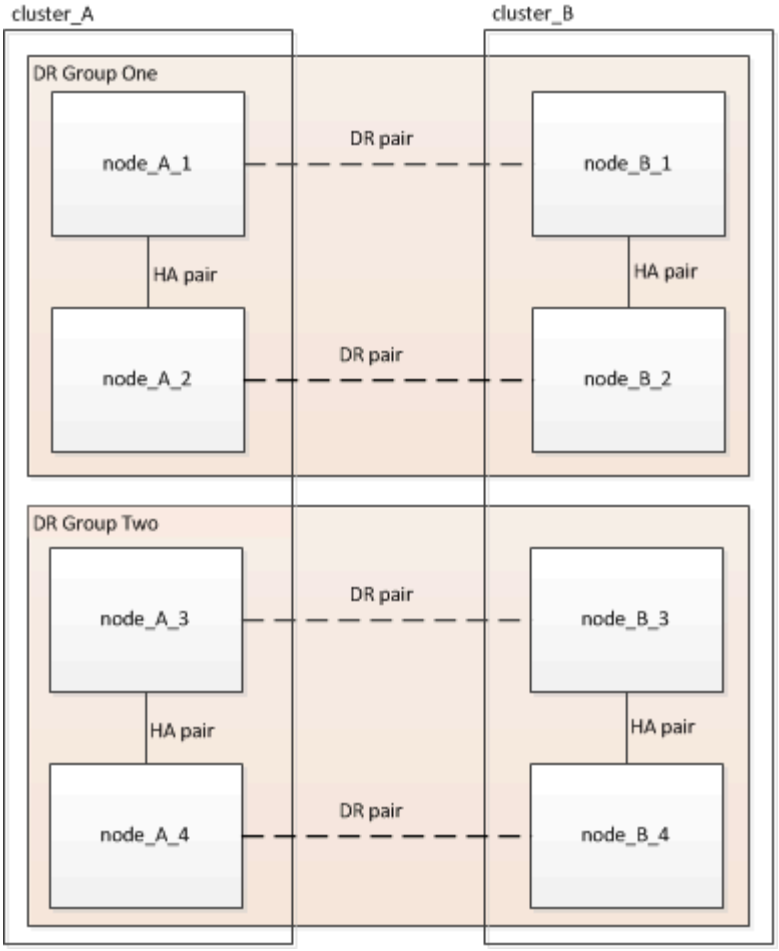
A partir do ONTAP 9.8, é possível remover um grupo de DR de uma configuração MetroCluster de oito nós para criar uma configuração MetroCluster de quatro nós.

Este procedimento é suportado no ONTAP 9.8 e posterior. Para sistemas que executam o ONTAP 9.7 ou anterior, consulte o artigo da base de dados de Conhecimento

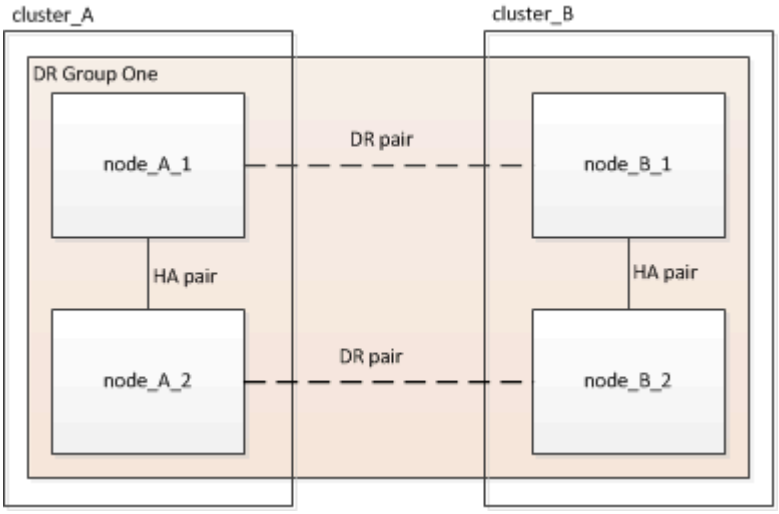
"Como remover um grupo de DR de uma configuração do MetroCluster"

"Suporte à NetApp"

Uma configuração de oito nós inclui oito nós organizados como dois grupos de RD de quatro nós.



Ao remover um grupo de DR, quatro nós permanecem na configuração.



Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a

criação de casos durante a atividade de manutenção.

Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Remoção dos nós do grupo de DR de cada cluster

Antes de começar

- É necessário executar esta etapa em ambos os clusters.
- O `metrocluster remove-dr-group` comando é suportado apenas no ONTAP 9.8 e posterior.

Passos

1. Prepare-se para a remoção do grupo DR, se ainda não o fez.

   a. Mover todos os volumes de dados para outro grupo de recuperação de desastres.

   b. Se o grupo de DR a ser removido contiver volumes de espelhamento de compartilhamento de carga, eles não poderão ser movidos. Crie novamente todos os volumes de espelhamento de compartilhamento de carga em outro grupo de DR e exclua os volumes de espelhamento de compartilhamento de carga no grupo de DR a serem removidos.

   c. Mova todos os volumes de metadados MDV_CRS para outro grupo DR seguindo o "Movimentação de um volume de metadados nas configurações do MetroCluster" procedimento.

   d. Exclua todos os volumes de metadados MDV_aud que possam existir no grupo DR a serem removidos.

   e. Exclua todos os agregados de dados no grupo DR a serem removidos, como mostrado no exemplo a seguir:

   ```
   ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
   -fields aggregate ,node
   ClusterA::> aggr delete -aggregate aggregate_name
   ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
   -fields aggregate ,node
   ClusterB::> aggr delete -aggregate aggregate_name
   ```

   Agregados raiz não são excluídos.

   f. Mova os LIFs de dados off-line.
   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin down`

   g. Migre todas as LIFs de dados para nós iniciais em outro grupo de DR. E
   `network interface show -home-node` *`old_node`*

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-node` *`new_node`*
   `-home-port` *`port-id`*

h. Mova os LIFs de dados de volta online.
`network interface modify -vserver *svm-name* -lif *data-lif* -status-admin up`

i. Migre o LIF de gerenciamento de cluster para um nó inicial em outro grupo de DR.

```
network interface show -role cluster-mgmt

network interface modify -vserver svm-name -lif cluster_mgmt -home-node
new_node -home-port port-id
```

O gerenciamento de nós e LIFs entre clusters não são migrados.

a. Transfira o epsilon para um nó em outro grupo DR, se necessário.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identifique e remova o grupo de DR.

a. Identifique o grupo DR correto para remoção:

```
metrocluster node show
```

b. Remova os nós do grupo de DR
`metrocluster remove-dr-group -dr-group-id 1`

O exemplo a seguir mostra a remoção da configuração do grupo DR no cluster_A.

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B"to remove the remote nodes in the DR
group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not completed
on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Repita a etapa anterior no cluster de parceiros.
4. Se estiver em uma configuração IP do MetroCluster, remova as conexões MetroCluster nos nós do grupo de DR antigo.

   Esses comandos podem ser emitidos de qualquer cluster e aplicados a todo o grupo de DR que abrange ambos os clusters.

   a. Desligar as ligações:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Exclua as interfaces MetroCluster nos nós do antigo grupo DR:

```
metrocluster configuration-settings interface delete
```

c. Exclua a configuração do antigo grupo DR. E
`metrocluster configuration-settings dr-group delete`

5. Desmarque os nós no grupo DR antigo.

Você deve executar esta etapa em cada cluster.

a. Defina o nível de privilégio avançado:

```
set -privilege advanced
```

b. Desativar o failover de armazenamento:

```
storage failover modify -node node-name -enable false
```

c. Unjoin the node
`cluster unjoin -node node-name`

Repita esta etapa para o outro nó local no grupo DR antigo.

d. Defina o nível de privilégio de administrador
`set -privilege admin`

6. Reative a HA do cluster no novo grupo de DR:

```
cluster ha modify -configured true
```

Você deve executar esta etapa em cada cluster.

7. Pare, desligue e remova os antigos módulos de controladora e compartimentos de storage.

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Documentação do MetroCluster"	• Todas as informações do MetroCluster

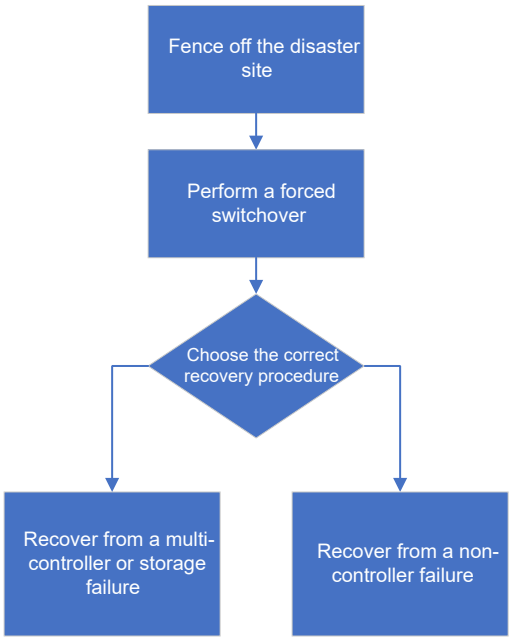
"Instalação e configuração do MetroCluster conectado à malha"	• Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do Stretch MetroCluster"	• Arquitetura Stretch MetroCluster • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster e recuperação de desastres"	• Compreender a configuração do MetroCluster • Switchover, cura e switchback • Recuperação de desastres
"Mantenha os componentes do MetroCluster"	• Diretrizes para manutenção em uma configuração MetroCluster FC • Procedimentos de substituição ou atualização de hardware e atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conetada à malha • Substituição de hardware em um local de desastre em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.

"Atualização, transição e expansão do MetroCluster"	• Atualizando ou atualizando uma configuração do MetroCluster • Transição de uma configuração MetroCluster FC para uma configuração MetroCluster IP • Expansão de uma configuração do MetroCluster com a adição de nós adicionais
"Instalação e configuração do software MetroCluster Tiebreaker"	• Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
"Documentação dos sistemas de hardware da ONTAP" Os procedimentos de manutenção padrão do compartimento de armazenamento podem ser usados com configurações IP do MetroCluster.	• Adição automática de um compartimento de disco • Remoção automática de um compartimento de disco
"Transição baseada em cópia"	• Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
"Conceitos de ONTAP"	• Como os agregados espelhados funcionam

Recuperar de um desastre

Fluxo de trabalho para recuperação de desastres

Use o fluxo de trabalho para executar a recuperação de desastres.



Realizar um switchover forçado após um desastre

Se ocorrer um desastre, há etapas que você deve executar no cluster de desastre e no cluster sobrevivente após o switchover para garantir um serviço de dados seguro e contínuo.

Determinar se ocorreu um desastre é feito por:

- Um administrador
- O software tiebreaker do MetroCluster, se estiver configurado
- O software Mediador ONTAP, se estiver configurado

Esgrima fora do local do desastre

Após o desastre, se os nós do local de desastre precisarem ser substituídos, é preciso impedi-los de retomar o serviço. Caso contrário, você arrisca a possibilidade de corrupção de dados se os clientes começarem a acessar os nós antes que o procedimento de substituição seja concluído.

Passo

1. Interrompa os nós no local de desastre e mantenha-os desligados ou no prompt DO Loader até que sejam direcionados para inicializar o ONTAP:

   ```
   system node halt -node disaster-site-node-name
   ```

Se os nós do local de desastre tiverem sido destruídos ou não puderem ser interrompidos, desligue a energia dos nós e não inicialize os nós de substituição até que sejam direcionados para o procedimento de recuperação.

Realizar uma comutação forçada

O processo de switchover, além de fornecer operações ininterruptas durante o teste e a manutenção, permite que você se recupere de uma falha no local com um único comando.

Antes de começar

- Pelo menos um dos nós do local sobreviventes deve estar ativo e em execução antes de executar o switchover.
- Todas as alterações de configuração anteriores devem ser concluídas antes de executar uma operação de switchback.

  Isto destina-se a evitar a concorrência com a operação de comutação negociada ou de comutação.

> As configurações do SnapMirror e do SnapVault são excluídas automaticamente.

Sobre esta tarefa

O `metrocluster switchover` comando alterna entre os nós em todos os grupos de DR na configuração MetroCluster. Por exemplo, em uma configuração de MetroCluster de oito nós, ele alterna entre os nós em ambos os grupos de DR.

Passos

1. Execute o switchover executando o seguinte comando no local sobrevivente:

   ```
   metrocluster switchover -forced-on-disaster true
   ```

   > A operação pode demorar um período de minutos para ser concluída. Você pode verificar o progresso usando o `metrocluster operation show` comando.

2. Responda `y` quando solicitado para continuar com o switchover.
3. Verifique se o switchover foi concluído com sucesso executando o `metrocluster operation show` comando.

```
mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

Se o switchover for vetado, você tem a opção de reemitir o `metrocluster switchover-forced-on-disaster true` comando com `--override-vetoes` a opção. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos virtuais que impediram o switchover.

Depois de terminar

Os relacionamentos do SnapMirror precisam ser restabelecidos após o switchover.

A saída para o comando storage Aggregate plex show é indeterminada após um switchover do MetroCluster

Quando você executa o `storage aggregate plex show` comando após um switchover MetroCluster, o status de plex0 do agregado raiz comutada é indeterminado e é exibido como falhou. Durante este tempo, a raiz comutada não é atualizada. O estado real deste Plex só pode ser determinado após a fase de cicatrização do MetroCluster.

Acessar volumes no estado NVFAIL após um switchover

Após um switchover, você deve limpar o estado NVFAIL redefinindo o `-in-nvfailed-state` parâmetro `volume modify` do comando para remover a restrição de clientes para acessar dados.

Antes de começar

O banco de dados ou o sistema de arquivos não deve estar em execução ou tentando acessar o volume afetado.

Sobre esta tarefa

A definição `-in-nvfailed-state` do parâmetro requer privilégios de nível avançado.

Passo

1. Recupere o volume usando o `volume modify` comando com o `-in-nvfailed-state` parâmetro definido como false.

Depois de terminar

Para obter instruções sobre como examinar a validade do arquivo de banco de dados, consulte a documentação do seu software de banco de dados específico.

Se o banco de dados usar LUNs, revise as etapas para tornar os LUNs acessíveis ao host após uma falha do NVRAM.

Informações relacionadas

"Monitoramento e proteção da validade do banco de dados usando NVFAIL"

Escolher o procedimento de recuperação correto

Após uma falha em uma configuração do MetroCluster, você deve selecionar o procedimento de recuperação correto. Use a tabela a seguir e os exemplos para selecionar o procedimento de recuperação apropriado.

Esta informação nesta tabela pressupõe que a instalação ou transição está concluída, o que significa que o `metrocluster configure` comando foi executado com sucesso.

Escopo das falhas no local de desastre	Procedimento
• Sem falha de hardware	"Recuperando-se de uma falha não controladora"
• Nenhuma falha no módulo do controlador • Outro hardware falhou	"Recuperando-se de uma falha não controladora"
• Falha ou falha de um único módulo de controlador de componentes FRU dentro do módulo do controlador • As unidades não falharam	Se uma falha for limitada a um único módulo de controlador, você deve usar o procedimento de substituição FRU do módulo de controlador para o modelo de plataforma. Em uma configuração de MetroCluster de quatro ou oito nós, essa falha é isolada para o par de HA local. **Nota:** o procedimento de substituição FRU do módulo do controlador pode ser usado em uma configuração MetroCluster de dois nós se não houver falhas de unidade ou outras falhas de hardware. "Documentação dos sistemas de hardware da ONTAP"
• Falha ou falha de um único módulo de controlador de componentes FRU dentro do módulo do controlador • As unidades falharam	"Recuperando-se de uma falha de vários controladores ou de armazenamento"
• Falha ou falha de um único módulo de controlador de componentes FRU dentro do módulo do controlador • As unidades não falharam • O hardware adicional fora do módulo do controlador falhou	"Recuperando-se de uma falha de vários controladores ou de armazenamento" Você deve ignorar todas as etapas para atribuição de unidade.

• Falha de vários módulos de controladora (com ou sem falhas adicionais) em um grupo de DR	"Recuperando-se de uma falha de vários controladores ou de armazenamento"

Cenários de falha do módulo do controlador durante a instalação do MetroCluster

Responder a uma falha do módulo do controlador durante o procedimento de configuração do MetroCluster depende se o `metrocluster configure` comando foi concluído com êxito.

- Se o `metrocluster configure` comando ainda não foi executado ou falhou, você deve reiniciar o procedimento de configuração do software MetroCluster desde o início com um módulo de controlador de substituição.

> Você deve ter certeza de executar as etapas em em "Restaurar padrões do sistema em um módulo do controlador"cada controlador (incluindo o controlador de substituição) para verificar se a configuração anterior foi removida.

- Se o `metrocluster configure` comando tiver sido concluído com êxito e o módulo do controlador falhar, utilize a tabela anterior para determinar o procedimento de recuperação correto.

Cenários de falha do módulo do controlador durante a transição MetroCluster FC para IP

O procedimento de recuperação pode ser usado se ocorrer uma falha no local durante a transição. No entanto, ela só pode ser usada se a configuração for uma configuração mista estável, com o grupo de DR FC e o grupo de DR IP totalmente configurados. A saída `metrocluster node show` do comando deve mostrar ambos os grupos de DR com todos os oito nós.

> Se a falha ocorreu durante a transição quando os nós estão em processo de serem adicionados ou removidos, você deve entrar em Contato com o suporte técnico.

Cenários de falha do módulo do controlador em configurações de MetroCluster de oito nós

Cenários de falha:

- Falhas de módulo único de controladora em um único grupo de DR
- Duas falhas no módulo de controladora em um único grupo de DR
- Falhas de módulo único de controladora em grupos de DR separados
- Três falhas no módulo do controlador distribuídas pelos grupos de DR

Falhas de módulo único de controladora em um único grupo de DR

Nesse caso, a falha é limitada a um par de HA.

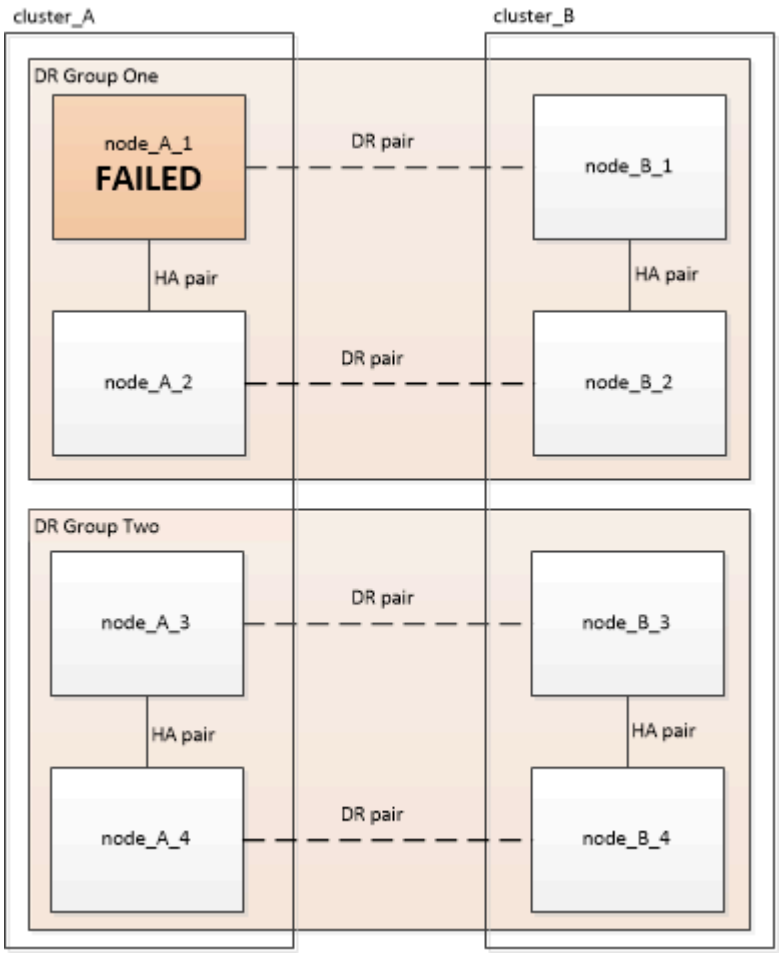
- Se nenhum armazenamento exigir substituição, você pode usar o procedimento de substituição FRU do módulo do controlador para o modelo da plataforma.

  "Documentação dos sistemas de hardware da ONTAP"

- Se o armazenamento necessitar de substituição, pode utilizar o procedimento de recuperação do módulo multi-controlador.

  "Recuperando-se de uma falha de vários controladores ou de armazenamento"

  Esse cenário também se aplica a configurações de MetroCluster de quatro nós.

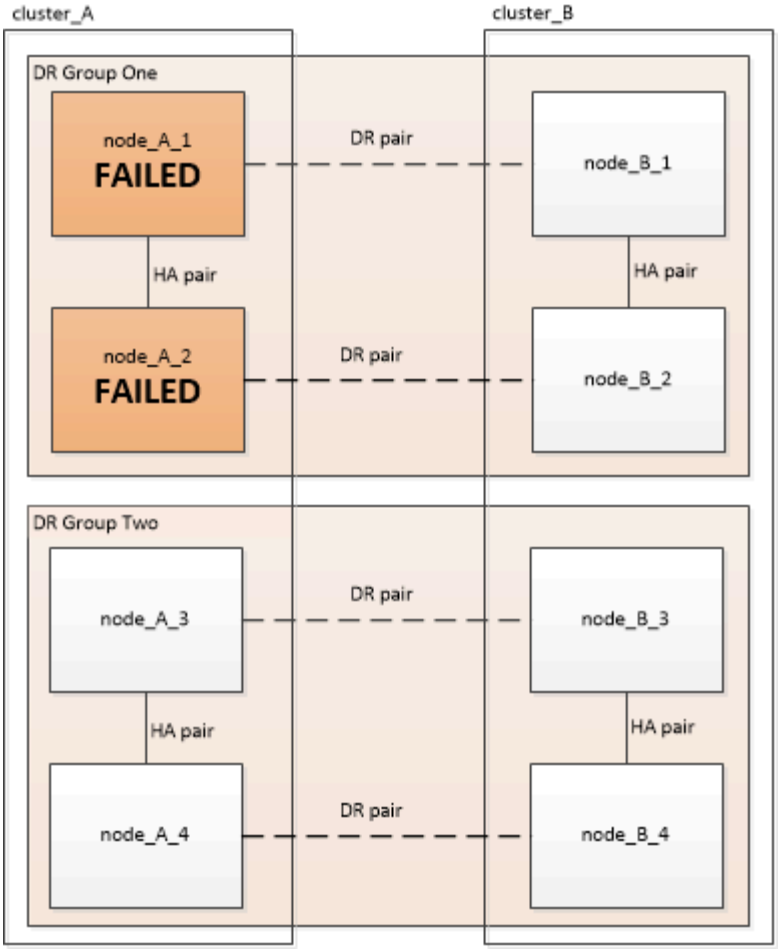


Duas falhas no módulo de controladora em um único grupo de DR

Neste caso, a falha requer uma mudança. Pode utilizar o procedimento de recuperação de falhas do módulo multi-controlador.

"Recuperando-se de uma falha de vários controladores ou de armazenamento"

Esse cenário também se aplica a configurações de MetroCluster de quatro nós.



Falhas de módulo único de controladora em grupos de DR separados

Nesse caso, a falha é limitada a pares de HA separados.

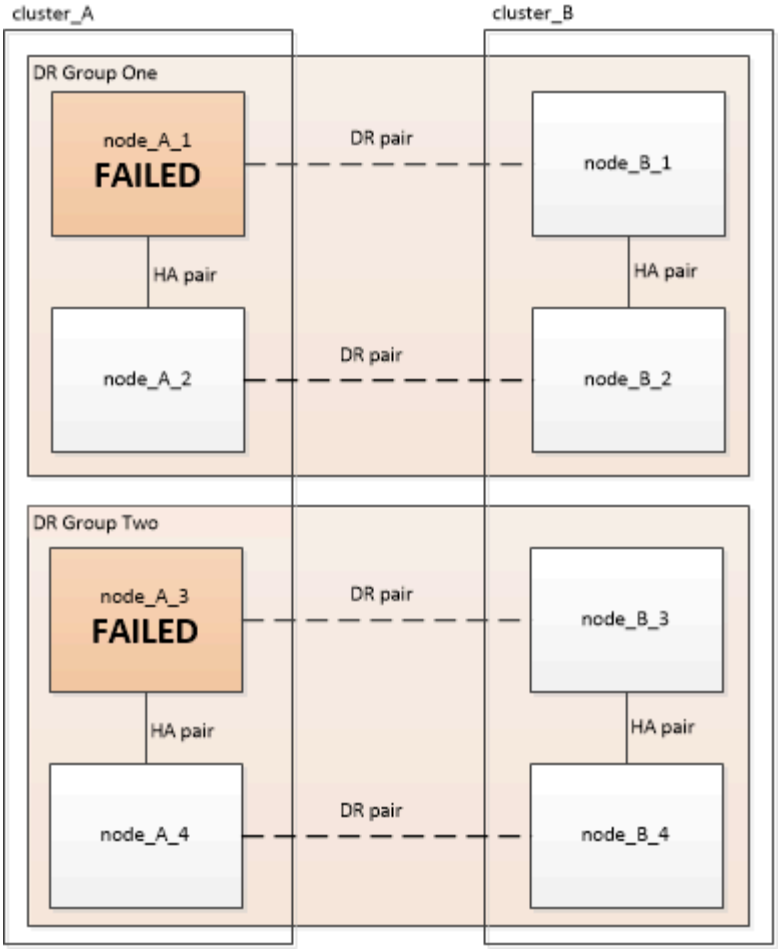
- Se nenhum armazenamento exigir substituição, você pode usar o procedimento de substituição FRU do módulo do controlador para o modelo da plataforma.

  O procedimento de substituição da FRU é realizado duas vezes, uma para cada módulo do controlador com falha.

  "Documentação dos sistemas de hardware da ONTAP"

- Se o armazenamento necessitar de substituição, pode utilizar o procedimento de recuperação do módulo multi-controlador.

  "Recuperando-se de uma falha de vários controladores ou de armazenamento"



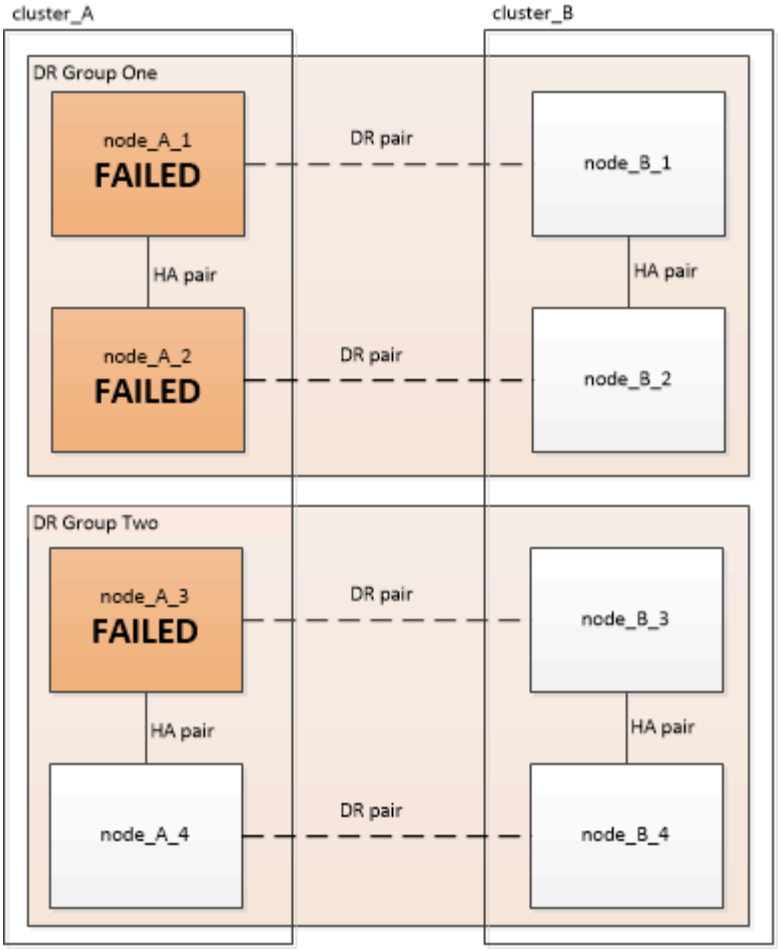
Três falhas no módulo do controlador distribuídas pelos grupos de DR

Neste caso, a falha requer uma mudança. Você pode usar o procedimento de recuperação de falha do módulo de vários controladores para o Grupo de RD 1.

"Recuperando-se de uma falha de vários controladores ou de armazenamento"

Você pode usar o procedimento de substituição FRU do módulo do controlador específico da plataforma para o Grupo dois de RD.

"Documentação dos sistemas de hardware da ONTAP"



Cenários de falha do módulo do controlador em configurações de MetroCluster de dois nós

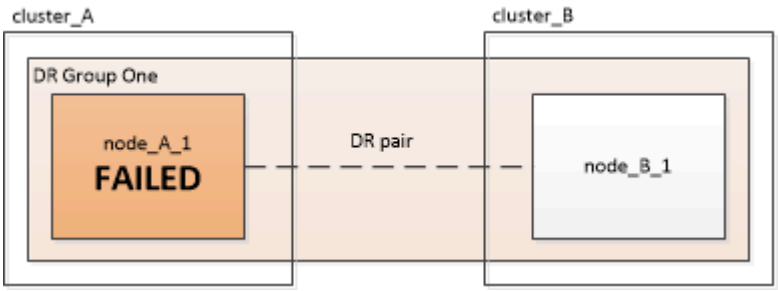
O procedimento utilizado depende da extensão da falha.

- Se nenhum armazenamento exigir substituição, você pode usar o procedimento de substituição FRU do módulo do controlador para o modelo da plataforma.

  "Documentação dos sistemas de hardware da ONTAP"

- Se o armazenamento necessitar de substituição, pode utilizar o procedimento de recuperação do módulo multi-controlador.

  "Recuperando-se de uma falha de vários controladores ou de armazenamento"



Recuperar de uma falha de vários controladores ou armazenamento

Recuperando-se de uma falha de vários controladores ou de armazenamento

Se a falha da controladora se estender a todos os módulos de controladora de um lado de um grupo de DR em uma configuração MetroCluster (incluindo um único controlador em uma configuração de MetroCluster de dois nós) ou o storage tiver sido substituído, você precisará substituir o equipamento e reatribuir a propriedade das unidades para recuperação do desastre.

Verifique se você verificou e executou as seguintes tarefas antes de usar este procedimento:

- Reveja os procedimentos de recuperação disponíveis antes de decidir utilizar este procedimento.

  "Escolher o procedimento de recuperação correto"

- Confirme se o registo da consola está ativado nos seus dispositivos.

  "Ativar o registo da consola"

- Certifique-se de que o local do desastre esteja vedado.

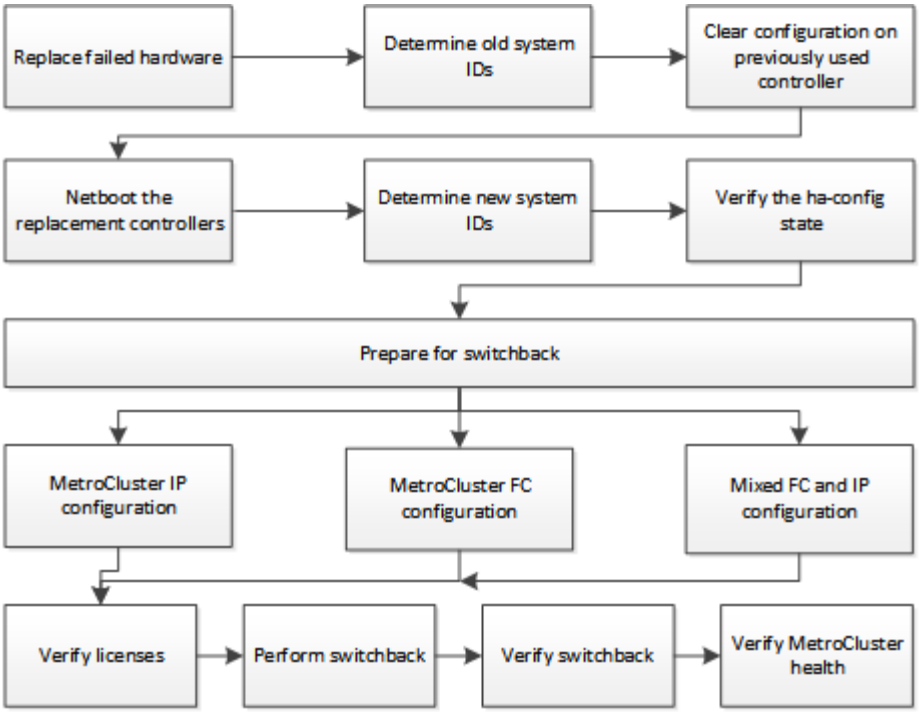
  "Esgrima fora do local do desastre".

- Verifique se o switchover foi realizado.

  "Realizar uma comutação forçada".

- Verifique se as unidades de substituição e os módulos do controlador são novos e não devem ter sido atribuídos propriedade anteriormente.
- Os exemplos deste procedimento mostram configurações de dois ou quatro nós. Se você tiver uma configuração de oito nós (dois grupos de DR), terá que levar em conta todas as falhas e executar a tarefa de recuperação necessária nos módulos adicionais da controladora.

Este procedimento utiliza o seguinte fluxo de trabalho:



Este procedimento pode ser usado ao executar a recuperação em um sistema que estava em transição intermediária quando a falha ocorreu. Nesse caso, você deve executar as etapas apropriadas ao se preparar para o switchback, como indicado no procedimento.

Ativar o registo da consola

Ative o log do console em seus dispositivos antes de continuar a substituir o hardware e inicializar novos controladores.

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Substitua o hardware e inicialize novos controladores

Se os componentes de hardware tiverem de ser substituídos, tem de os substituir utilizando os respetivos guias de instalação e substituição de hardware individuais.

Substitua o hardware no local de desastre

Antes de começar

Os controladores de armazenamento devem ser desligados ou permanecer parados (mostrando o prompt Loader).

Passos

1. Substitua os componentes conforme necessário.

> Nesta etapa, você substitui e faz o cabeamento dos componentes exatamente como eles foram cabeados antes do desastre. Não deve ligar os componentes.

Se você está substituindo…	Execute estas etapas…	Usando estes guias…
Switches FC em uma configuração MetroCluster FC	a. Instale os novos interrutores. b. Faça o cabo das ligações ISL. Não ligue os switches FC no momento.	"Mantenha os componentes do MetroCluster"
Switches IP em uma configuração IP MetroCluster	a. Instale os novos interrutores. b. Faça o cabo das ligações ISL. Não ligue os interrutores IP neste momento.	"Instalação e configuração do IP MetroCluster: Diferenças entre as configurações do ONTAP MetroCluster"
Compartimentos de disco	a. Instale as gavetas de disco e os discos. ◦ As pilhas de compartimentos de disco devem ser a mesma configuração que no local que sobreviveu. ◦ Os discos podem ser do mesmo tamanho ou maiores, mas devem ser do mesmo tipo (SAS ou SATA). b. Faça o cabeamento das gavetas de disco para gavetas adjacentes na stack e para a ponte FC para SAS. Não ligue as gavetas de disco no momento.	"Documentação dos sistemas de hardware da ONTAP"
Cabos SAS	a. Instale os novos cabos. Não ligue as gavetas de disco no momento.	"Documentação dos sistemas de hardware da ONTAP"

Pontes FC para SAS em uma configuração de MetroCluster FC	a. Instalar as pontes FC para SAS. b. Faça cabos das pontes FC para SAS. Vincule-os aos switches FC ou aos módulos do controlador, dependendo do tipo de configuração do MetroCluster. Não ligue as pontes FC para SAS no momento.	"Instalação e configuração do MetroCluster conectado à malha" "Instalação e configuração do Stretch MetroCluster"

Módulos do controlador	a. Instale os novos módulos do controlador: ◦ Os módulos do controlador têm de ser o mesmo modelo que os que estão a ser substituídos. Por exemplo, os módulos do controlador 8080 devem ser substituídos por módulos do controlador 8080. ◦ Os módulos do controlador não devem ter sido anteriormente parte de qualquer cluster dentro da configuração do MetroCluster ou de qualquer configuração de cluster existente anteriormente. Se eles fossem, você deve definir padrões e executar um processo de wipeconfig.. ◦ Certifique-se de que todas as placas de interface de rede (como Ethernet ou FC) estejam nos mesmos slots usados nos módulos de controladora antigos. b. Faça o cabo dos novos módulos de controlador exatamente o mesmo que os antigos. As portas que conetam o módulo da controladora ao storage (por conexões com os switches IP ou FC, pontes FC para SAS ou diretamente) devem ser as mesmas que as usadas antes do desastre. Não ligue os módulos do controlador neste momento.	"Documentação dos sistemas de hardware da ONTAP"

2. Verifique se todos os componentes estão cabeados corretamente para sua configuração.

- "Configuração IP do MetroCluster"
- "Configuração conectado à malha do MetroCluster"

Determine as IDs do sistema e as IDs de VLAN dos módulos antigos do controlador

Depois de substituir todo o hardware no local de desastre, você deve determinar as IDs do sistema dos módulos do controlador substituídos. Você precisa dos IDs de sistema antigos quando reatribuir discos aos novos módulos do controlador. Se os sistemas forem modelos AFF A220, AFF A250, AFF A400, AFF A800, FAS2750, FAS500f, FAS8300 ou FAS8700, você também deverá determinar as IDs de VLAN usadas pelas interfaces IP do MetroCluster.

Antes de começar

Todos os equipamentos no local de desastre devem ser desligados.

Sobre esta tarefa

Esta discussão fornece exemplos para configurações de dois e quatro nós. Para configurações de oito nós, você precisa levar em conta todas as falhas nos nós adicionais no segundo grupo de DR.

Para uma configuração de MetroCluster de dois nós, você pode ignorar referências ao segundo módulo de controlador em cada local.

Os exemplos deste procedimento baseiam-se nas seguintes premissas:

- O local A é o local do desastre.
- Node_A_1 falhou e está sendo completamente substituído.
- Node_A_2 falhou e está sendo completamente substituído.

  O nó _A_2 está presente apenas em uma configuração MetroCluster de quatro nós.

- O local B é o local sobrevivente.
- Node_B_1 está em bom estado.
- Node_B_2 está em bom estado.

  Node_B_2 está presente apenas em uma configuração MetroCluster de quatro nós.

Os módulos do controlador têm as seguintes IDs de sistema originais:

Número de nós na configuração do MetroCluster	Nó	ID do sistema original
Quatro	node_A_1	4068741258
node_A_2	4068741260	node_B_1
4068741254	node_B_2	4068741256
Dois	node_A_1	4068741258

Passos

1. No site sobrevivente, exiba as IDs do sistema dos nós na configuração do MetroCluster.

Número de nós na configuração do MetroCluster	Use este comando
Quatro ou oito	`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`
Dois	`metrocluster node show -fields node-systemid,dr-partner-systemid`

Neste exemplo para uma configuração de MetroCluster de quatro nós, as seguintes IDs de sistema antigas são recuperadas:

- Node_A_1: 4068741258
- Node_A_2: 4068741260

Os discos pertencentes aos módulos de controladora antigos ainda são de propriedade desses IDs de sistema.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  4068741258    4068741260
4068741254          4068741256
1           Cluster_A  Node_A_2  4068741260    4068741258
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

Neste exemplo para uma configuração de MetroCluster de dois nós, o seguinte ID de sistema antigo é recuperado:

- Node_A_1: 4068741258

Os discos pertencentes ao antigo módulo do controlador ainda são propriedade desta ID do sistema.

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1  4068741258    4068741254
1           Cluster_B  Node_B_1  -             -
2 entries were displayed.
```

2. Para configurações IP do MetroCluster usando o serviço Mediador ONTAP, obtenha o endereço IP do serviço Mediador ONTAP:

   ```
   storage iscsi-initiator show -node * -label mediator
   ```

3. Se os sistemas forem modelos AFF A220, AFF A400, FAS2750, FAS8300 ou FAS8700, determine as IDs de VLAN:

   ```
   metrocluster interconnect show
   ```

   Os IDs de VLAN estão incluídos no nome do adaptador mostrado na coluna adaptador da saída.

   Neste exemplo, os IDs de VLAN são 120 e 130:

```
metrocluster interconnect show
                         Mirror   Mirror
                 Partner Admin    Oper
Node Partner Name Type    Status   Status  Adapter Type   Status
---- ------------ ------- -------- ------- ------- ------ ------
Node_A_1 Node_A_2 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
Node_A_2 Node_A_1 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
12 entries were displayed.
```

Isolar unidades de substituição do local sobrevivente (configurações IP do MetroCluster)

Você deve isolar quaisquer unidades de substituição retirando as conexões do iniciador iSCSI da MetroCluster dos nós sobreviventes.

Sobre esta tarefa

Este procedimento só é necessário nas configurações IP do MetroCluster.

Passos

1. A partir do prompt de qualquer nó sobrevivente, altere para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

   Você precisa responder com `y` quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

2. Desconete os iniciadores iSCSI em ambos os nós sobreviventes no grupo DR:

   ```
   storage iscsi-initiator disconnect -node surviving-node -label *
   ```

   Este comando deve ser emitido duas vezes, uma para cada um dos nós sobreviventes.

   O exemplo a seguir mostra os comandos para desconetar os iniciadores no local B:

   ```
   site_B::*> storage iscsi-initiator disconnect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator disconnect -node node_B_2 -label *
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Limpe a configuração de um módulo do controlador

Antes de usar um novo módulo de controlador na configuração do MetroCluster, você deve limpar a configuração existente.

Passos

1. Se necessário, interrompa o nó para exibir o prompt Loader:

   ```
   halt
   ```

2. No prompt Loader, defina as variáveis ambientais como valores padrão:

   ```
   set-defaults
   ```

3. Salvar o ambiente:

   ```
   saveenv
   ```

4. No prompt DO Loader, inicie o menu de inicialização:

```
boot_ontap menu
```

5. No prompt do menu de inicialização, desmarque a configuração:

   ```
   wipeconfig
   ```

   Responda `yes` ao prompt de confirmação.

   O nó reinicializa e o menu de inicialização é exibido novamente.

6. No menu de inicialização, selecione a opção **5** para inicializar o sistema no modo Manutenção.

   Responda `yes` ao prompt de confirmação.

Netboot os novos módulos do controlador

Se os novos módulos do controlador tiverem uma versão diferente do ONTAP da versão nos módulos do controlador sobreviventes, você deverá inicializar os novos módulos do controlador.

Antes de começar

- Você deve ter acesso a um servidor HTTP.
- Você deve ter acesso ao site de suporte da NetApp para baixar os arquivos de sistema necessários para sua plataforma e versão do software ONTAP que está sendo executado nele.

  "Suporte à NetApp"

Passos

1. Acesse o "Site de suporte da NetApp" para baixar os arquivos usados para executar o netboot do sistema.
2. Transfira o software ONTAP adequado a partir da secção de transferência de software do site de suporte da NetApp e guarde o ficheiro ONTAP-version_image.tgz num diretório acessível à Web.
3. Vá para o diretório acessível pela Web e verifique se os arquivos que você precisa estão disponíveis.

Se o modelo da plataforma for…	Então…
Sistemas da série FAS/AFF8000	Extraia o conteúdo do arquivo ONTAP-version_image.tgzfile para o diretório de destino: Tar -zxvf ONTAP-version_image.tgz NOTA: Se você estiver extraindo o conteúdo no Windows, use 7-Zip ou WinRAR para extrair a imagem netboot. Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel:netboot/kernel
Todos os outros sistemas	Sua lista de diretórios deve conter uma pasta netboot com um arquivo do kernel: ONTAP-version_image.tgz você não precisa extrair o arquivo ONTAP-version_image.tgz.

4. No prompt Loader, configure a conexão netboot para um LIF de gerenciamento:
   - Se o endereçamento IP for DHCP, configure a conexão automática:

     ```
     ifconfig e0M -auto
     ```

- Se o endereçamento IP for estático, configure a conexão manual:

  ```
  ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
  ```

5. Execute o netboot.
   - Se a plataforma for um sistema da série 80xx, use este comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se a plataforma for qualquer outro sistema, use o seguinte comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
     ```

6. No menu de arranque, selecione a opção **(7) Instalar primeiro o novo software** para transferir e instalar a nova imagem de software no dispositivo de arranque.

   ```
    Disregard the following message: "This procedure is not supported for Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive upgrades of software, not to upgrades of controllers.
   . Se você for solicitado a continuar o procedimento, digite `y` e, quando solicitado a fornecer o pacote, digite o URL do arquivo de imagem: `\http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Certifique-se de entrar `n` para ignorar a recuperação de backup quando você vir um prompt semelhante ao seguinte:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Reinicie entrando `y` quando você vir um prompt semelhante ao seguinte:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

9. No menu Boot (Inicialização), selecione **opção 5** para entrar no modo Maintenance (Manutenção).
10. Se tiver uma configuração de MetroCluster de quatro nós, repita este procedimento no outro novo módulo do controlador.

Determine as IDs do sistema dos módulos do controlador de substituição

Depois de substituir todo o hardware no local de desastre, você deve determinar a ID do sistema do módulo ou módulos do controlador de armazenamento recém-instalados.

Sobre esta tarefa

Deve executar este procedimento com os módulos do controlador de substituição no modo de manutenção.

Esta seção fornece exemplos para configurações de dois e quatro nós. Para configurações de dois nós, você pode ignorar referências ao segundo nó em cada local. Para configurações de oito nós, você deve ter em conta os nós adicionais no segundo grupo de DR. Os exemplos fazem as seguintes suposições:

- O local A é o local do desastre.
- O nó_A_1 foi substituído.
- O nó_A_2 foi substituído.

  Presente apenas em configurações de MetroCluster de quatro nós.

- O local B é o local sobrevivente.
- Node_B_1 está em bom estado.
- Node_B_2 está em bom estado.

  Presente apenas em configurações de MetroCluster de quatro nós.

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Número de nós na configuração do MetroCluster	Nó	ID do sistema original	Nova ID do sistema	O parecerá com esse nó como parceiro de recuperação de desastres
Quatro	node_A_1	4068741258	1574774970	node_B_1
node_A_2	4068741260	1574774991	node_B_2	node_B_1
4068741254	inalterado	node_A_1	node_B_2	4068741256
inalterado	node_A_2	Dois	node_A_1	4068741258
1574774970	node_B_1	node_B_1	4068741254	inalterado

Em uma configuração de MetroCluster de quatro nós, o sistema determina as parcerias de DR emparelhando o nó com o ID de sistema mais baixo no site_A e o nó com o ID de sistema mais baixo no site_B. Como as IDs do sistema mudam, os pares de DR podem ser diferentes após a conclusão das substituições do controlador do que eram antes do desastre.

No exemplo anterior:

- Node_A_1 (1574774970) será emparelhado com node_B_1 (4068741254)
- Node_A_2 (1574774991) será emparelhado com node_B_2 (4068741256)

Passos

1. Com o nó no modo Manutenção, exiba a ID do sistema local do nó de cada nó: `disk show`

   No exemplo a seguir, o novo ID do sistema local é 1574774970:

   ```
   *> disk show
    Local System ID: 1574774970
    ...
   ```

2. No segundo nó, repita a etapa anterior.

   Esta etapa não é necessária em uma configuração de MetroCluster de dois nós.

   No exemplo a seguir, o novo ID do sistema local é 1574774991:

   ```
   *> disk show
    Local System ID: 1574774991
    ...
   ```

Verifique o estado ha-config dos componentes

Em uma configuração MetroCluster, o estado ha-config do módulo do controlador e dos componentes do chassi deve ser definido como "mcc" ou "MCC-2n" para que eles iniciem corretamente.

Antes de começar

O sistema tem de estar no modo de manutenção.

Sobre esta tarefa

Esta tarefa deve ser executada em cada novo módulo do controlador.

Passos

1. No modo de manutenção, apresentar o estado HA do módulo do controlador e do chassis:

   `ha-config show`

   O estado de HA correto depende da configuração do MetroCluster.

Número de controladores na configuração MetroCluster	O estado HA para todos os componentes deve ser…
Configuração de FC MetroCluster de oito ou quatro nós	mcc
Configuração de FC MetroCluster de dois nós	mcc-2n
Configuração IP do MetroCluster	mccip

2. Se o estado do sistema apresentado do controlador não estiver correto, defina o estado HA para o módulo

do controlador:

Número de controladores na configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify controller mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify controller mcc-2n`
Configuração IP do MetroCluster	`ha-config modify controller mccip`

3. Se o estado do sistema apresentado do chassis não estiver correto, defina o estado HA para o chassis:

Número de controladores na configuração MetroCluster	Comando
Configuração de FC MetroCluster de oito ou quatro nós	`ha-config modify chassis mcc`
Configuração de FC MetroCluster de dois nós	`ha-config modify chassis mcc-2n`
Configuração IP do MetroCluster	`ha-config modify chassis mccip`

4. Repita estas etapas no outro nó de substituição.

Determine se a criptografia de ponta a ponta foi ativada nos sistemas originais

Você deve verificar se os sistemas originais foram configurados para criptografia de ponta a ponta.

Passo

1. Execute o seguinte comando a partir do site sobrevivente:

   `metrocluster node show -fields is-encryption-enabled`

   Se a encriptação estiver ativada, é apresentada a seguinte saída:

```
1 cluster_A node_A_1 true
1 cluster_A node_A_2 true
1 cluster_B node_B_1 true
1 cluster_B node_B_2 true
4 entries were displayed.
```

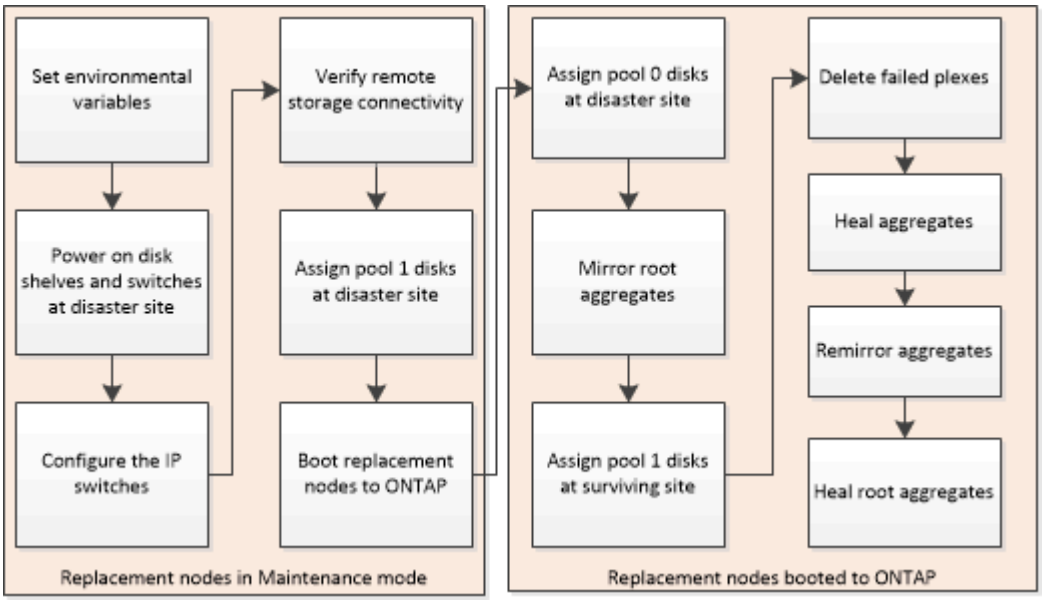
> "Configurar criptografia de ponta a ponta"Consulte para obter informações sobre os sistemas suportados.

Prepare-se para switchback em uma configuração IP MetroCluster

Prepare-se para switchback em uma configuração IP MetroCluster

Você deve executar certas tarefas para preparar a configuração IP do MetroCluster para a operação de switchback.

Sobre esta tarefa



Definição das variáveis ambientais necessárias nas configurações IP do MetroCluster

Nas configurações IP do MetroCluster, você deve recuperar o endereço IP das interfaces MetroCluster nas portas Ethernet e usá-las para configurar as interfaces nos módulos de controladora de substituição.

Sobre esta tarefa

- Esta tarefa é necessária apenas nas configurações IP do MetroCluster.
- Os comandos nesta tarefa são executados a partir do prompt de cluster do local sobrevivente e do prompt Loader dos nós no local de desastre.
- Certas plataformas usam uma VLAN para a interface IP do MetroCluster. Por padrão, cada uma das duas portas usa uma VLAN diferente: 10 e 20.

  Se suportado, você também pode especificar uma VLAN diferente (não padrão) maior que 100 (entre 101 e 4095) usando o `vlan-id` parâmetro.

  As seguintes plataformas **não** suportam o `vlan-id` parâmetro:

  - FAS8200 e AFF A300
  - AFF A320
  - FAS9000 e AFF A700

◦ AFF C800, ASA C800, AFF A800 e ASA A800

Todas as outras plataformas suportam o `vlan-id` parâmetro.

- Os nós nestes exemplos têm os seguintes endereços IP para suas conexões IP MetroCluster:

> Estes exemplos são para um sistema AFF A700 ou FAS9000. As interfaces variam de acordo com o modelo da plataforma.

Nó	Porta	Endereço IP
node_A_1	e5a	172.17.26.10
e5b	172.17.27.10	node_A_2
e5a	172.17.26.11	e5b
172.17.27.11	node_B_1	e5a
172.17.26.13	e5b	172.17.27.13
node_B_2	e5a	172.17.26.12

A tabela a seguir resume as relações entre os nós e os endereços IP MetroCluster de cada nó.

Nó	Parceiro DE HA	Parceiro de DR	Parceiro auxiliar DR
node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12
node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13
node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11
node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10

Passos

1. A partir do site sobrevivente, reúna os endereços IP das interfaces MetroCluster no local de desastre:

   ```
   metrocluster configuration-settings connection show
   ```

   Os endereços necessários são os endereços do parceiro DR mostrados na coluna **Endereço de rede de destino**.

   A saída do comando varia dependendo do modelo da plataforma.

Sistemas introduzidos no ONTAP 9.15,1 ou posterior

Os sistemas introduzidos no ONTAP 9.15,1 ou posterior (AFF A70, AFF A90 e AFF A1K) têm portas separadas para HA e DR, como mostrado na saída de exemplo a seguir:

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

Todos os outros sistemas

A saída a seguir mostra os endereços IP de uma configuração com sistemas AFF A700 e FAS9000 com as interfaces IP MetroCluster nas portas E5A e e5b. As interfaces podem variar dependendo do tipo de plataforma.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
```

```
12 entries were displayed.
```

2. Se você precisar determinar o ID da VLAN ou o endereço de gateway para a interface, determine os IDs da VLAN do local sobrevivente:

   `metrocluster configuration-settings interface show`

   - Você precisa determinar a ID da VLAN se os modelos da plataforma suportarem IDs de VLAN (consulte a lista acima) e se você não estiver usando os IDs de VLAN padrão.
   - Você precisa do endereço de gateway se estiver usando "Redes de área ampla da camada 3"o .

     Os IDs de VLAN estão incluídos na coluna **Endereço de rede** da saída. A coluna **Gateway** mostra o endereço IP do gateway.

     Neste exemplo, as interfaces são e0a com a VLAN ID 120 e e0b com a VLAN ID 130:

```
Cluster-A::*> metrocluster configuration-settings interface show
DR
Config
Group Cluster Node     Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1
      cluster_A
              node_A_1
                  Home Port: e0a-120
                          172.17.26.10  255.255.255.0  -
completed
                  Home Port: e0b-130
                          172.17.27.10  255.255.255.0  -
completed
```

3. No prompt DO Loader para cada um dos nós do local de desastre, defina o valor do bootarg dependendo do modelo da plataforma:

   - Se as interfaces estiverem usando as VLANs padrão ou o modelo de plataforma não usar um ID de VLAN (consulte a lista acima), o *vlan-id* não será necessário.
   - Se a configuração não estiver usando "Layer3 redes de grande área", o valor para *gateway-IP-address* será **0** (zero).

Sistemas introduzidos no ONTAP 9.15,1 ou posterior

O valor para *HA-Partner-IP-address* deve ser definido como **0** (zero) em sistemas introduzidos no ONTAP 9.15,1 ou posterior porque eles têm portas separadas para DR e HA.

Defina o seguinte bootarg:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-
address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-
address,DR-aux-partnerIP-address,vlan-id
```

Os comandos a seguir definem os valores para node_A_1 usando VLAN 120 para a primeira rede e VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir mostra os comandos para node_A_1 sem um ID de VLAN:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

Todos os outros sistemas

Defina o seguinte bootarg:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-
address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-
address,DR-aux-partnerIP-address,vlan-id
```

Os comandos a seguir definem os valores para node_A_1 usando VLAN 120 para a primeira rede e

VLAN 130 para a segunda rede:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

O exemplo a seguir mostra os comandos para node_A_1 sem um ID de VLAN:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

4. A partir do local sobrevivente, reúna os UUIDs para o local de desastre:

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid

  (metrocluster node show)
dr-group-id cluster     node     node-uuid
node-cluster-uuid
----------- ----------- -------- -------------------------------------
------------------------------
1           cluster_A   node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_A   node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_B   node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098

c9e55d
1           cluster_B   node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098

c9e55d
4 entries were displayed.
cluster_A::*>
```

Nó	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	a9a7a7a-9a81-11e7-a4e9-00a098908c35

5. No prompt Loader dos nós de substituição, defina os UUIDs:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID`
```

a. Defina os UUIDs em node_A_1.

O exemplo a seguir mostra os comandos para definir os UUIDs em node_A_1:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f

setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Defina os UUIDs em node_A_2:

O exemplo a seguir mostra os comandos para definir os UUIDs em node_A_2:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f

setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d

setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

6. Se os sistemas originais foram configurados para ADP, em cada prompt DO Loader dos nós de

substituição, ative o ADP:

```
setenv bootarg.mcc.adp_enabled true
```

7. Se estiver executando o ONTAP 9.5, 9,6 ou 9,7, em cada prompt do Loader dos nós de substituição, ative a seguinte variável:

```
setenv bootarg.mcc.lun_part true
```

   a. Defina as variáveis em node_A_1.

      O exemplo a seguir mostra os comandos para definir os valores em node_A_1 ao executar o ONTAP 9.6:

      ```
      setenv bootarg.mcc.lun_part true
      ```

   b. Defina as variáveis em node_A_2.

      O exemplo a seguir mostra os comandos para definir os valores em node_A_2 ao executar o ONTAP 9.6:

```
setenv bootarg.mcc.lun_part true
```

8. Se os sistemas originais foram configurados para criptografia de ponta a ponta, em cada prompt DO Loader dos nós de substituição, defina o seguinte bootarg:

```
setenv bootarg.mccip.encryption_enabled 1
```

9. Se os sistemas originais foram configurados para ADP, em cada um dos prompt Loader dos nós de substituição, defina o ID do sistema original (**not** a ID do sistema do módulo do controlador de substituição) e o ID do sistema do parceiro DR do nó:

```
setenv bootarg.mcc.local_config_id original-sysID

setenv bootarg.mcc.dr_partner dr_partner-sysID
```

   "Determine as IDs do sistema dos módulos do controlador antigos"

   a. Defina as variáveis em node_A_1.

      O exemplo a seguir mostra os comandos para definir as IDs do sistema em node_A_1:

      - O ID do sistema antigo de node_A_1 é 4068741258.
      - A ID do sistema do node_B_1 é 4068741254.

        ```
        setenv bootarg.mcc.local_config_id 4068741258
        setenv bootarg.mcc.dr_partner 4068741254
        ```

   b. Defina as variáveis em node_A_2.

O exemplo a seguir mostra os comandos para definir as IDs do sistema em node_A_2:

- O ID do sistema antigo de node_A_1 é 4068741260.
- A ID do sistema do node_B_1 é 4068741256.

```
setenv bootarg.mcc.local_config_id 4068741260
setenv bootarg.mcc.dr_partner 4068741256
```

Ligar o equipamento no local de desastre (configurações IP do MetroCluster)

É necessário ligar os componentes dos compartimentos de disco e dos switches IP MetroCluster no local de desastre. Os módulos do controlador no local de desastre permanecem no prompt DO Loader.

Sobre esta tarefa

Os exemplos deste procedimento assumem o seguinte:

- O local A é o local do desastre.
- O local B é o local sobrevivente.

Passos

1. Ligue as gavetas de disco no local de desastre e verifique se todos os discos estão em execução.
2. Ligue os switches IP MetroCluster se eles ainda não estiverem ligados.

Configurar os switches IP (configurações IP do MetroCluster)

Você deve configurar todos os switches IP que foram substituídos.

Sobre esta tarefa

Esta tarefa aplica-se apenas às configurações IP do MetroCluster.

Isso deve ser feito em ambos os interrutores. Depois de configurar o primeiro switch, verifique se o acesso ao armazenamento no site sobrevivente não é afetado.

> Você não deve prosseguir com o segundo switch se o acesso ao armazenamento no site sobrevivente for afetado.

Passos

1. "Instalação e configuração IP do MetroCluster: : Diferenças entre as configurações do ONTAP MetroCluster"Consulte para obter os procedimentos de cabeamento e configuração de um switch de substituição.

   Você pode usar os procedimentos nas seções a seguir:

   - Cabeamento dos switches IP
   - Configurar os switches IP
2. Se os ISLs foram desativados no site sobrevivente, ative os ISLs e verifique se os ISLs estão online.

a. Ative as interfaces ISL no primeiro interrutor:

```
no shutdown
```

Os exemplos a seguir mostram os comandos de um switch IP Broadcom ou de um switch IP Cisco.

Fornecedor de switch	Comandos
Broadcom	(IP_Switch_A_1)> enable (IP_switch_A_1)# configure (IP_switch_A_1)(Config)# interface 0/13-0/16 (IP_switch_A_1)(Interface 0/13-0/16)# no shutdown (IP_switch_A_1)(Interface 0/13-0/16)# exit (IP_switch_A_1)(Config)# exit
Cisco	IP_switch_A_1# conf t IP_switch_A_1(config)# int eth1/15-eth1/20 IP_switch_A_1(config)# no shutdown IP_switch_A_1(config)# copy running startup IP_switch_A_1(config)# show interface brief

b. Ative as interfaces ISL no switch parceiro:

```
no shutdown
```

Os exemplos a seguir mostram os comandos de um switch IP Broadcom ou de um switch IP Cisco.

Fornecedor de switch	Comandos

Broadcom	(IP_Switch_A_2)> enable (IP_switch_A_2)# configure (IP_switch_A_2)(Config)# interface 0/13-0/16 (IP_switch_A_2)(Interface 0/13- 0/16)# no shutdown (IP_switch_A_2)(Interface 0/13- 0/16)# exit (IP_switch_A_2)(Config)# exit
Cisco	IP_switch_A_2# conf t IP_switch_A_2(config)# int eth1/15-eth1/20 IP_switch_A_2(config)# no shutdown IP_switch_A_2(config)# copy running startup IP_switch_A_2(config)# show interface brief

c. Verifique se as interfaces estão ativadas:

   `show interface brief`

   O exemplo a seguir mostra a saída de um switch Cisco.

```
IP_switch_A_2(config)# show interface brief

--------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------
mt0 -- up 10.10.99.10 100 1500
--------------------------------------------------------------
Ethernet    VLAN Type Mode    Status Reason Speed   Port
Interface                                         Ch
#
--------------------------------------------------------------
.
.
.
Eth1/15    10   eth   access  up     none   40G(D)  --
Eth1/16    10   eth   access  up     none   40G(D)  --
Eth1/17    10   eth   access  down   none   auto(D) --
Eth1/18    10   eth   access  down   none   auto(D) --
Eth1/19    10   eth   access  down   none   auto(D) --
Eth1/20    10   eth   access  down   none   auto(D) --
.
.
.
IP_switch_A_2#
```

Verificar a conetividade do armazenamento ao local remoto (configurações IP do MetroCluster)

Você precisa confirmar se os nós substituídos têm conectividade com as gavetas de disco no local que sobreviveu.

Sobre esta tarefa

Essa tarefa é realizada nos nós de substituição no local de desastre.

Esta tarefa é executada no modo Manutenção.

Passos

1. Exiba os discos que são de propriedade da ID do sistema original.

   ```
   disk show -s old-system-ID
   ```

   Os discos remotos podem ser reconhecidos pelo dispositivo 0m. 0m indica que o disco está ligado através da ligação iSCSI MetroCluster. Esses discos devem ser reatribuídos posteriormente no procedimento de recuperação.

```
*> disk show -s 4068741256
Local System ID: 1574774970

  DISK     OWNER                  POOL   SERIAL NUMBER   HOME
DR HOME
---------- --------------------- ----- -------------
--------------------- ----------------------
0m.i0.0L11 node_A_2 (4068741256) Pool1 S396NA0HA02128  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.1L38 node_A_2 (4068741256) Pool1 S396NA0J148778  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.0L52 node_A_2 (4068741256) Pool1 S396NA0J148777  node_A_2
(4068741256) node_A_2  (4068741256)
...
...
NOTE: Currently 49 disks are unowned. Use 'disk show -n' for additional
information.
*>
```

2. Repita esta etapa nos outros nós de substituição

Reatribuir a propriedade do disco para discos do pool 1 no local de desastre (configurações IP do MetroCluster)

Se um ou ambos os módulos da controladora ou placas NVRAM tiverem sido substituídos no local de desastre, o ID do sistema foi alterado e você deve reatribuir discos pertencentes aos agregados raiz aos módulos da controladora de substituição.

Sobre esta tarefa

Como os nós estão no modo de switchover, apenas os discos que contêm os agregados raiz de pool1 do local de desastre serão reatribuídos nesta tarefa. Eles são os únicos discos ainda possuídos pelo ID do sistema antigo neste momento.

Essa tarefa é realizada nos nós de substituição no local de desastre.

Esta tarefa é executada no modo Manutenção.

Os exemplos fazem as seguintes suposições:

- O local A é o local do desastre.
- O nó_A_1 foi substituído.
- O nó_A_2 foi substituído.
- O local B é o local sobrevivente.
- Node_B_1 está em bom estado.
- Node_B_2 está em bom estado.

Os IDs de sistema antigo e novo foram identificados no "Substitua o hardware e inicialize novos

controladores".

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Nó	ID do sistema original	Nova ID do sistema
node_A_1	4068741258	1574774970
node_A_2	4068741260	1574774991
node_B_1	4068741254	inalterado
node_B_2	4068741256	inalterado

Passos

1. Com o nó de substituição no modo Manutenção, reatribua os discos agregados raiz, usando o comando correto, dependendo se o sistema está configurado com ADP e a versão do ONTAP.

   Você pode prosseguir com a reatribuição quando solicitado.

Se o sistema estiver usando ADP…	Use este comando para reatribuição de disco…
Sim (ONTAP 9.8)	`disk reassign -s old-system-ID -d new-system-ID -r dr-partner-system-ID`
Sim (ONTAP 9.7.x e anterior)	`disk reassign -s old-system-ID -d new-system-ID -p old-partner-system-ID`
Não	`disk reassign -s old-system-ID -d new-system-ID`

   O exemplo a seguir mostra a reatribuição de unidades em um sistema que não seja ADP:

```
*> disk reassign -s 4068741256 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537037643.
Do you want to continue (y/n)? y
disk reassign parameters: new_home_owner_id 537070473 ,
new_home_owner_name
Disk 0m.i0.3L14 will be reassigned.
Disk 0m.i0.1L6 will be reassigned.
Disk 0m.i0.1L8 will be reassigned.
Number of disks to be reassigned: 3
```

2. Destruir o conteúdo dos discos da caixa de correio:

   `mailbox destroy local`

   Você pode prosseguir com a operação destruir quando solicitado.

   O exemplo a seguir mostra a saída para o comando local destruir caixa de correio:

```
*> mailbox destroy local
Destroying mailboxes forces a node to create new empty mailboxes,
which clears any takeover state, removes all knowledge
of out-of-date plexes of mirrored volumes, and will prevent
management services from going online in 2-node cluster
HA configurations.
Are you sure you want to destroy the local mailboxes? y
..............Mailboxes destroyed.
*>
```

3. Se os discos tiverem sido substituídos, haverá falha nos plexes locais que devem ser excluídos.

   a. Exibir o status agregado:

      `aggr status`

      No exemplo a seguir, o Plex node_A_1_aggr0/plex0 falhou.

```
*> aggr status
Aug 18 15:00:07 [node_B_1:raid.vol.mirror.degraded:ALERT]: Aggregate
node_A_1_aggr0 is
   mirrored and one plex has failed. It is no longer protected by
mirroring.
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex0
   clean(-1), online(0)
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex2
   clean(0), online(1)
Aug 18 15:00:07 [node_B_1:raid.mirror.vote.noRecord1Plex:error]:
WARNING: Only one plex
   in aggregate node_A_1_aggr0 is available. Aggregate might contain
stale data.
Aug 18 15:00:07 [node_B_1:raid.debug:info]:
volobj_mark_sb_recovery_aggrs: tree:
   node_A_1_aggr0 vol_state:1 mcc_dr_opstate: unknown
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (VOL):
   raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (MIRROR):
   raid state change UNINITD -> DEGRADED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex0
   (PLEX): raid state change UNINITD -> FAILED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2
   (PLEX): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2/rg0
   (GROUP): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Topology updated for
aggregate node_A_1_aggr0
   to plex plex2
*>
```

b. Eliminar o Plex com falha:

`aggr destroy plex-id`

```
*> aggr destroy node_A_1_aggr0/plex0
```

4. Interrompa o nó para exibir o prompt DO Loader:

   `halt`

5. Repita essas etapas no outro nó no local do desastre.

Inicializando no ONTAP em módulos de controlador de substituição em configurações IP do MetroCluster

Você precisa inicializar os nós de substituição no local de desastre para o sistema operacional ONTAP.

Sobre esta tarefa

Esta tarefa começa com os nós no local de desastre no modo Manutenção.

Passos

1. Em um dos nós de substituição, saia para o prompt Loader: `halt`
2. Apresentar o menu de arranque: `boot_ontap menu`
3. No menu de inicialização, selecione a opção 6, **Atualizar flash a partir da configuração de backup**.

   O sistema arranca duas vezes. Você deve responder `yes` quando solicitado a continuar. Após a segunda inicialização, você deve responder `y` quando solicitado sobre a incompatibilidade da ID do sistema.

   > Se você não tiver limpado o conteúdo do NVRAM de um módulo de controlador de substituição usado, poderá ver a seguinte mensagem de pânico: `PANIC: NVRAM contents are invalid…`. Se isso ocorrer, inicialize o sistema no prompt do ONTAP novamente (`boot_ontap menu`). Então você precisa Redefina os bootargs boot_recovery e rdb_corrupt

   - Confirmação para continuar prompt:

     ```
     Selection (1-9)? 6

     This will replace all flash-based configuration with the last backup
     to
     disks. Are you sure you want to continue?: yes
     ```

   - Aviso de incompatibilidade da ID do sistema:

     ```
     WARNING: System ID mismatch. This usually occurs when replacing a
     boot device or NVRAM cards!
     Override system ID? {y|n} y
     ```

4. No local que sobreviveu, verifique se as IDs de sistema do parceiro corretas foram aplicadas aos nós:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

Neste exemplo, os seguintes novos IDs de sistema devem aparecer na saída:

- Node_A_1: 1574774970
- Node_A_2: 1574774991

A coluna "ha-Partner-systemid" deve mostrar os novos IDs do sistema.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  1574774970    1574774991
4068741254          4068741256
1           Cluster_A  Node_A_2  1574774991    1574774970
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                    -
-
1           Cluster_B  Node_B_2  -             -                    -
-
4 entries were displayed.
```

5. Se as IDs do sistema do parceiro não foram definidas corretamente, você deve definir manualmente o valor correto:
   a. Interrompa e exiba o prompt Loader no nó.
   b. Verifique o valor atual do bootarg do Partner-sysID:

      ```
      printenv
      ```

   c. Defina o valor para a ID correta do sistema do parceiro:

      ```
      setenv partner-sysid partner-sysID
      ```

   d. Inicialize o nó:

      ```
      boot_ontap
      ```

   e. Repita essas subetapas no outro nó, se necessário.
6. Confirme se os nós de substituição no local de desastre estão prontos para o switchback:

   ```
   metrocluster node show
   ```

   Os nós de substituição devem estar aguardando o modo de recuperação de switchback. Se eles estiverem no modo normal, você pode reinicializar os nós de substituição. Após essa inicialização, os nós devem estar aguardando o modo de recuperação de switchback.

O exemplo a seguir mostra que os nós de substituição estão prontos para switchback:

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

7. Verifique as configurações da conexão MetroCluster:

   `metrocluster configuration-settings connection show`

   O estado de configuração deve indicar Concluído.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
```

```
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.10    DR Partner
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.11    DR Auxiliary
completed
             node_B_1
                Home Port: e5a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.11    DR Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.10    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.11    DR Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.10    DR Auxiliary
completed
      cluster_A
             node_A_2
                Home Port: e5a
                     172.17.26.11    172.17.26.10    HA Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.12    DR Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.13    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.10    HA Partner
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.12    DR Partner
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.13    DR Auxiliary
completed
```

```
              node_A_1
                 Home Port: e5a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.13    DR Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.12    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.13    DR Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.12    DR Auxiliary
completed
24 entries were displayed.

cluster_B::*>
```

8. Repita as etapas anteriores no outro nó no local do desastre.

Reponha os bootargs boot_recovery e rdb_corrupt

Se necessário, você pode redefinir o boot_recovery e o rdb_corrupt_bootargs

Passos

1. Interrompa o nó de volta ao prompt DO Loader:

```
node_A_1::*> halt -node _node-name_
```

2. Verifique se os seguintes bootargs foram definidos:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se qualquer bootarg tiver sido definido como um valor, desconfigure-o e inicie o ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Restaurar a conetividade dos nós sobreviventes para o local de desastre (configurações IP do MetroCluster)

Você deve restaurar as conexões do iniciador iSCSI MetroCluster dos nós sobreviventes.

Sobre esta tarefa

Este procedimento só é necessário nas configurações IP do MetroCluster.

Passos

1. A partir do prompt de qualquer nó sobrevivente, altere para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

   Você precisa responder com `y` quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

2. Conete os iniciadores iSCSI em ambos os nós sobreviventes no grupo DR:

   ```
   storage iscsi-initiator connect -node surviving-node -label *
   ```

   O exemplo a seguir mostra os comandos para conetar os iniciadores no local B:

   ```
   site_B::*> storage iscsi-initiator connect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator connect -node node_B_2 -label *
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Verificando a atribuição automática ou atribuindo manualmente unidades de pool 0

Em sistemas configurados para ADP, você deve verificar se as unidades do pool 0 foram atribuídas automaticamente. Em sistemas que não estão configurados para ADP, você deve atribuir manualmente as unidades 0 do pool.

Verificar a atribuição de unidades de pool 0 em sistemas ADP no local de desastre (sistemas IP MetroCluster)

Se as unidades tiverem sido substituídas no local de desastre e o sistema estiver configurado para ADP, você deverá verificar se as unidades remotas estão visíveis para os nós e foram atribuídas corretamente.

Passo

1. Verifique se as unidades do pool 0 são atribuídas automaticamente:

```
disk show
```

No exemplo a seguir para um sistema AFF A800 sem compartimentos externos, um quarto (8 unidades) foi atribuído automaticamente ao node_A_1 e um quarto foi atribuído automaticamente ao node_A_2. As unidades restantes serão unidades remotas (pool1) para node_B_1 e node_B_2.

```
cluster_A::*> disk show
                  Usable     Disk      Container           Container
Disk              Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_A_1
node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
```

```
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Atribuição de unidades de pool 0 em sistemas não ADP no local de desastre (configurações IP MetroCluster)

Se as unidades tiverem sido substituídas no local de desastre e o sistema não estiver configurado para ADP, será necessário atribuir manualmente novas unidades ao pool 0.

Sobre esta tarefa

Para sistemas ADP, as unidades são atribuídas automaticamente.

Passos

1. Em um dos nós de substituição no local de desastre, reatribua as unidades 0 do pool de nós:

   `storage disk assign -n number-of-replacement disks -p 0`

   Este comando atribui as unidades recém-adicionadas (e não possuídas) no local de desastre. Você deve atribuir o mesmo número e tamanho (ou maior) de unidades que o nó teve antes do desastre. A `storage disk assign` página man contém mais informações sobre a execução de atribuição de unidade mais granular.

2. Repita a etapa no outro nó de substituição no local de desastre.

Atribuição de unidades de pool 1 no local sobrevivente (configurações IP do MetroCluster)

Se as unidades tiverem sido substituídas no local de desastre e o sistema não estiver configurado para ADP, no local sobrevivente, você precisará atribuir manualmente unidades remotas localizadas no local de desastre ao pool de nós sobreviventes 1. Você deve identificar o número de unidades a serem atribuídas.

Sobre esta tarefa

Para sistemas ADP, as unidades são atribuídas automaticamente.

Passo

1. No local sobrevivente, atribua as unidades 1 (remotas) do primeiro nó: `storage disk assign -n number-of-replacement disks -p 1 0m*`

Este comando atribui as unidades recém-adicionadas e não possuídas no local de desastre.

O seguinte comando atribui 22 unidades:

```
cluster_B::> storage disk assign -n 22 -p 1 0m*
```

Exclusão de plexes com falha de propriedade do site sobrevivente (configurações IP do MetroCluster)

Depois de substituir o hardware e atribuir discos, você deve excluir plexes remotos com falha que são de propriedade dos nós do local sobreviventes, mas localizados no local de desastre.

Sobre esta tarefa

Estas etapas são executadas no cluster sobrevivente.

Passos

1. Identificar os agregados locais:
`storage aggregate show -is-home true`

```
cluster_B::> storage aggregate show -is-home true

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB 95% online       1 node_B_1
raid4,

mirror

degraded
node_B_2_aggr0 1.49TB  74.12GB 95% online       1 node_B_2
raid4,

mirror

degraded
node_B_1_aggr1 2.99TB  2.88TB   3% online      15 node_B_1
raid_dp,

mirror

degraded
node_B_1_aggr2 2.99TB  2.91TB   3% online      14 node_B_1
```

```
raid_tec,

mirror

degraded
node_B_2_aggr1 2.95TB  2.80TB   5% online      37 node_B_2
raid_dp,

mirror

degraded
node_B_2_aggr2 2.99TB  2.87TB   4% online      35 node_B_2
raid_tec,

mirror

degraded
6 entries were displayed.

cluster_B::>
```

2. Identificar os plexes remotos com falha:

   `storage aggregate plex show`

   O exemplo a seguir chama os plexes que são remotos (não plex0) e têm um status de "failed" (Falha):

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_1_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr2 plex0 normal,active true     0
node_B_1_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr2 plex0 normal,active true     0
node_B_2_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
20 entries were displayed.

cluster_B::>
```

3. Fique offline cada um dos plexes com falha e, em seguida, exclua-os:

   a. Fique offline os plexes com falha:

      `storage aggregate plex offline -aggregate aggregate-name -plex plex-id`

      O exemplo a seguir mostra o agregado "node_B_2_aggr1/plex1" sendo colocado offline:

      ```
      cluster_B::> storage aggregate plex offline -aggregate node_B_1_aggr0
      -plex plex4

      Plex offline successful on plex: node_B_1_aggr0/plex4
      ```

   b. Eliminar o Plex com falha:

      `storage aggregate plex delete -aggregate aggregate-name -plex plex-id`

      Você pode destruir o Plex quando solicitado.

O exemplo a seguir mostra o Plex node_B_2_aggr1/plex1 sendo excluído.

```
cluster_B::> storage aggregate plex delete -aggregate  node_B_1_aggr0
-plex plex4

Warning: Aggregate "node_B_1_aggr0" is being used for the local
management root
         volume or HA partner management root volume, or has been
marked as
         the aggregate to be used for the management root volume
after a
         reboot operation. Deleting plex "plex4" for this aggregate
could lead
         to unavailability of the root volume after a disaster
recovery
         procedure. Use the "storage aggregate show -fields
         has-mroot,has-partner-mroot,root" command to view such
aggregates.

Warning: Deleting plex "plex4" of mirrored aggregate "node_B_1_aggr0"
on node
         "node_B_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you
want to
         destroy this plex? {y|n}: y
[Job 633] Job succeeded: DONE

cluster_B::>
```

Você deve repetir estas etapas para cada um dos plexos com falha.

4. Confirme se os plexos foram removidos:

```
storage aggregate plex show -fields aggregate,status,is-online,plex,pool
```

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

5. Identificar os agregados comutados:

   `storage aggregate show -is-home false`

   Você também pode usar o `storage aggregate plex show -fields aggregate,status,is-online,plex,pool` comando para identificar agregados comutados do Plex 0. Eles terão um status de "falhou, inativo".

   Os comandos a seguir mostram quatro agregados comutados:

   - node_A_1_aggr1
   - node_A_1_aggr2
   - node_A_2_aggr1
   - node_A_2_aggr2

```
cluster_B::> storage aggregate show -is-home false

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.12TB  1.88TB   11% online      91 node_B_1
raid_dp,

mirror

degraded
node_A_1_aggr2 2.89TB  2.64TB    9% online      90 node_B_1
raid_tec,

mirror

degraded
node_A_2_aggr1 2.12TB  1.86TB   12% online      91 node_B_2
raid_dp,

mirror

degraded
node_A_2_aggr2 2.89TB  2.64TB    9% online      90 node_B_2
raid_tec,

mirror

degraded
4 entries were displayed.

cluster_B::>
```

6. Identificar plexos comutados:

   `storage aggregate plex show -fields aggregate,status,is-online,Plex,pool`

   Você deseja identificar os plexes com um status de "falhou, inativo".

   Os comandos a seguir mostram quatro agregados comutados:

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

7. Eliminar o Plex com falha:

   `storage aggregate plex delete -aggregate node_A_1_aggr1 -plex plex0`

   Você pode destruir o Plex quando solicitado.

   O exemplo a seguir mostra o nó Plex_A_1_aggr1/plex0 sendo excluído:

```
cluster_B::> storage aggregate plex delete -aggregate node_A_1_aggr1
-plex plex0

Warning: Aggregate "node_A_1_aggr1" hosts MetroCluster metadata volume
         "MDV_CRS_e8457659b8a711e78b3b00a0988fe74b_A". Deleting plex
"plex0"
         for this aggregate can lead to the failure of configuration
         replication across the two DR sites. Use the "volume show
-vserver
         <admin-vserver> -volume MDV_CRS*" command to verify the
location of
         such volumes.

Warning: Deleting plex "plex0" of mirrored aggregate "node_A_1_aggr1" on
node
         "node_A_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you want
to
         destroy this plex? {y|n}: y
[Job 639] Job succeeded: DONE

cluster_B::>
```

Você deve repetir essas etapas para cada um dos agregados com falha.

8. Verifique se não há plexo com falha restante no local sobrevivente.

   A saída a seguir mostra que todos os plexes são normais, ativos e online.

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------ --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex1 normal,active true     1
10 entries were displayed.

cluster_B::>
```

Executar a recuperação de agregados e restaurar espelhos (configurações IP do MetroCluster)

Depois de substituir o hardware e atribuir discos, em sistemas que executam o ONTAP 9.5 ou anterior, você pode executar as operações de recuperação do MetroCluster. Em todas as versões do ONTAP, você deve confirmar se os agregados estão espelhados e, se necessário, reiniciar o espelhamento.

Sobre esta tarefa

A partir do ONTAP 9.6, as operações de recuperação são executadas automaticamente quando os nós do local de desastre são inicializados. Os comandos de cura não são necessários.

Estas etapas são executadas no cluster sobrevivente.

Passos

1. Se você estiver usando o ONTAP 9.6 ou posterior, verifique se a recuperação automática foi concluída com sucesso:

   a. Confirme se as operações heal-aggr-auto e heal-root-aggr-auto foram concluídas:

      ```
      metrocluster operation history show
      ```

      A saída a seguir mostra que as operações foram concluídas com êxito no cluster_A.

```
cluster_B::*> metrocluster operation history show
Operation                    State          Start Time       End
Time
---------------------------- -------------- ----------------
----------------
heal-root-aggr-auto          successful      2/25/2019 06:45:58

2/25/2019 06:46:02
heal-aggr-auto               successful     2/25/2019 06:45:48

2/25/2019 06:45:52
.
.
.
```

b. Confirme se o local de desastre está pronto para o switchback:

```
metrocluster node show
```

A saída a seguir mostra que as operações foram concluídas com êxito no cluster_A.

```
cluster_B::*> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   heal roots
completed
              node_A_2       configured     enabled   heal roots
completed
      cluster_B
              node_B_1       configured     enabled   waiting for
switchback recovery
              node_B_2       configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Se você estiver usando o ONTAP 9.5 ou anterior, será necessário executar a recuperação agregada:

a. Verifique o estado dos nós:

```
metrocluster node show
```

A saída a seguir mostra que o switchover foi concluído, de modo que a recuperação pode ser executada.

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_B
              node_B_1          configured     enabled   switchover
completed
              node_B_2          configured     enabled   switchover
completed
      cluster_A
              node_A_1          configured     enabled   waiting for
switchback recovery
              node_A_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

b. Execute a fase de cicatrização de agregados:

`metrocluster heal -phase aggregates`

A saída a seguir mostra uma operação típica de recuperação de agregados.

```
cluster_B::*> metrocluster heal -phase aggregates
[Job 647] Job succeeded: Heal Aggregates is successful.

cluster_B::*> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 10/26/2017 12:01:15
   End Time: 10/26/2017 12:01:17
     Errors: -

cluster_B::*>
```

c. Verifique se a recuperação agregada foi concluída e o local de desastre está pronto para o switchback:

`metrocluster node show`

A saída a seguir mostra que a fase "heal agreements" foi concluída no cluster_A.

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal
aggregates completed
              node_A_2           configured     enabled   heal
aggregates completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

3. Se os discos tiverem sido substituídos, você deve espelhar os agregados locais e comutados:

   a. Exibir os agregados:

      `storage aggregate show`

      ```
      cluster_B::> storage aggregate show
      cluster_B Aggregates:
      Aggregate     Size Available Used% State   #Vols  Nodes
      RAID Status
      --------- -------- --------- ----- ------- ------ ----------------
      ------------
      node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
      raid4,

      normal
      node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
      raid4,

      normal
      node_B_1_aggr1 3.14TB  3.04TB    3% online     15 node_B_1
      raid_dp,

      normal
      node_B_1_aggr2 3.14TB  3.06TB    3% online     14 node_B_1
      raid_tec,
      ```

```
normal
node_B_1_aggr1 3.14TB  2.99TB    5% online     37 node_B_2
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.02TB    4% online     35 node_B_2
raid_tec,

normal

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.36TB  2.12TB   10% online     91 node_B_1
raid_dp,

normal
node_A_1_aggr2 3.14TB  2.90TB    8% online     90 node_B_1
raid_tec,

normal
node_A_2_aggr1 2.36TB  2.10TB   11% online     91 node_B_2
raid_dp,

normal
node_A_2_aggr2 3.14TB  2.89TB    8% online     90 node_B_2
raid_tec,

normal
12 entries were displayed.

cluster_B::>
```

b. Espelhar o agregado:

```
storage aggregate mirror -aggregate aggregate-name
```

A saída a seguir mostra uma operação de espelhamento típica.

```
cluster_B::> storage aggregate mirror -aggregate node_B_1_aggr1

Info: Disks would be added to aggregate "node_B_1_aggr1" on node
"node_B_1" in
      the following manner:

      Second Plex

        RAID Group rg0, 6 disks (block checksum, raid_dp)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          dparity    5.20.6                    SSD
-
          parity     5.20.14                   SSD
-
          data       5.21.1                    SSD
894.0GB
          data       5.21.3                    SSD
894.0GB
          data       5.22.3                    SSD
894.0GB
          data       5.21.13                   SSD
894.0GB

      Aggregate capacity available for volume use would be 2.99TB.

Do you want to continue? {y|n}: y
```

c. Repita o passo anterior para cada um dos agregados do local sobrevivente.

d. Aguarde que os agregados sejam ressincronizados; você pode verificar o status com o `storage aggregate show` comando.

A saída a seguir mostra que vários agregados estão ressincronizando.

```
cluster_B::> storage aggregate show

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,
```

```
mirrored,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

mirrored,

normal
node_B_1_aggr1 2.86TB  2.76TB    4% online     15 node_B_1
raid_dp,

resyncing
node_B_1_aggr2 2.89TB  2.81TB    3% online     14 node_B_1
raid_tec,

resyncing
node_B_2_aggr1 2.73TB  2.58TB    6% online     37 node_B_2
raid_dp,

resyncing
node_B-2_aggr2 2.83TB  2.71TB    4% online     35 node_B_2
raid_tec,

resyncing

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 1.86TB  1.62TB   13% online     91 node_B_1
raid_dp,

resyncing
node_A_1_aggr2 2.58TB  2.33TB   10% online     90 node_B_1
raid_tec,

resyncing
node_A_2_aggr1 1.79TB  1.53TB   14% online     91 node_B_2
raid_dp,

resyncing
node_A_2_aggr2 2.64TB  2.39TB    9% online     90 node_B_2
raid_tec,
```

```
resyncing
12 entries were displayed.
```

e. Confirme se todos os agregados estão online e ressincronizados:

```
storage aggregate plex show
```

A saída a seguir mostra que todos os agregados foram ressincronizados.

```
cluster_A::> storage aggregate plex show
  ()
                    Is      Is         Resyncing
Aggregate Plex      Online  Resyncing    Percent Status
--------- --------- ------- ---------- --------- ---------------
node_B_1_aggr0 plex0 true    false              - normal,active
node_B_1_aggr0 plex8 true    false              - normal,active
node_B_2_aggr0 plex0 true    false              - normal,active
node_B_2_aggr0 plex8 true    false              - normal,active
node_B_1_aggr1 plex0 true    false              - normal,active
node_B_1_aggr1 plex9 true    false              - normal,active
node_B_1_aggr2 plex0 true    false              - normal,active
node_B_1_aggr2 plex5 true    false              - normal,active
node_B_2_aggr1 plex0 true    false              - normal,active
node_B_2_aggr1 plex9 true    false              - normal,active
node_B_2_aggr2 plex0 true    false              - normal,active
node_B_2_aggr2 plex5 true    false              - normal,active
node_A_1_aggr1 plex4 true    false              - normal,active
node_A_1_aggr1 plex8 true    false              - normal,active
node_A_1_aggr2 plex1 true    false              - normal,active
node_A_1_aggr2 plex5 true    false              - normal,active
node_A_2_aggr1 plex4 true    false              - normal,active
node_A_2_aggr1 plex8 true    false              - normal,active
node_A_2_aggr2 plex1 true    false              - normal,active
node_A_2_aggr2 plex5 true    false              - normal,active
20 entries were displayed.
```

4. Em sistemas que executam o ONTAP 9.5 e versões anteriores, execute a fase de recuperação de agregados raiz:

```
metrocluster heal -phase root-aggregates
```

```
cluster_B::> metrocluster heal -phase root-aggregates
[Job 651] Job is queued: MetroCluster Heal Root Aggregates Job.Oct 26
13:05:00
[Job 651] Job succeeded: Heal Root Aggregates is successful.
```

5. Verifique se a fase "heal Roots" foi concluída e o local de desastre está pronto para o switchback:

   A saída a seguir mostra que a fase "heal Roots" foi concluída no cluster_A.

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal roots
completed
              node_A_2           configured     enabled   heal roots
completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

Prossiga para verificar as licenças nos nós substituídos.

"Verificando licenças nos nós substituídos"

Prepare-se para o switchback em uma configuração MetroCluster FC

Verificação da configuração da porta (somente configurações MetroCluster FC)

Você deve definir as variáveis ambientais no nó e desligá-lo para prepará-lo para a configuração do MetroCluster.

Sobre esta tarefa

Este procedimento é executado com os módulos do controlador de substituição no modo de manutenção.

As etapas para verificar a configuração das portas são necessárias somente em sistemas nos quais as portas FC ou CNA são usadas no modo iniciador.

Passos

1. No modo Manutenção, restaure a configuração da porta FC:

   `ucadmin modify -m fc -t initiatoradapter_name`

   Se você quiser usar apenas um de um par de portas na configuração do iniciador, insira um nome preciso do adaptador.

2. Execute uma das seguintes ações, dependendo da configuração:

Se a configuração da porta FC for…	Então…
O mesmo para ambas as portas	Responda "y" quando solicitado pelo sistema, porque modificar uma porta em um par de portas também modifica a outra porta.
Diferente	a. Responda "n" quando solicitado pelo sistema. b. Restaure a configuração da porta FC: `ucadmin modify -m fc -t initiator

3. Sair do modo de manutenção:

   `halt`

   Depois de emitir o comando, aguarde até que o sistema pare no prompt DO Loader.

4. Inicialize o nó novamente no modo Manutenção para que as alterações de configuração entrem em vigor:

   `boot_ontap maint`

5. Verifique os valores das variáveis:

   `ucadmin show`

6. Saia do modo de manutenção e exiba o prompt Loader:

   `halt`

Configuração de pontes FC para SAS (somente configurações de MetroCluster FC)

Se você substituiu as pontes FC para SAS, será necessário configurá-las ao restaurar a configuração do MetroCluster. O procedimento é idêntico à configuração inicial de uma ponte FC-para-SAS.

Passos

1. Ligue as pontes FC para SAS.
2. Defina o endereço IP nas portas Ethernet utilizando o `set IPAddress port ipaddress` comando.
   - `port` Pode ser "MP1" ou "MP2".
   - `ipaddress` Pode ser um endereço IP no formato xxx.xxx.xxx.xxx.

No exemplo a seguir, o endereço IP é 10.10.10.55 na porta Ethernet 1:

```
Ready.
set IPAddress MP1 10.10.10.55

Ready. *
```

3. Defina a máscara de sub-rede IP nas portas Ethernet utilizando o `set IPSubnetMask port mask` comando.

   - `port` Pode ser "MP1" ou "MP2".
   - `mask` pode ser uma máscara de sub-rede no formato xxx.xxx.xxx.xxx.

   No exemplo a seguir, a máscara de sub-rede IP é 255.255.255.0 na porta Ethernet 1:

```
Ready.
set IPSubnetMask MP1 255.255.255.0

Ready. *
```

4. Defina a velocidade nas portas Ethernet utilizando o `set EthernetSpeed port speed` comando.

   - `port` Pode ser "MP1" ou "MP2".
   - `speed` pode ser "100" ou "1000".

   No exemplo a seguir, a velocidade Ethernet é definida como 1000 na porta Ethernet 1.

```
Ready.
set EthernetSpeed MP1 1000

Ready. *
```

5. Salve a configuração usando o `saveConfiguration` comando e reinicie a ponte quando solicitado a fazê-lo.

   Guardar a configuração depois de configurar as portas Ethernet permite-lhe prosseguir com a configuração da ponte utilizando Telnet e permite-lhe aceder à ponte utilizando FTP para efetuar atualizações de firmware.

   O exemplo a seguir mostra o `saveConfiguration` comando e o prompt para reiniciar a ponte.

```
Ready.
SaveConfiguration
  Restart is necessary....
  Do you wish to restart (y/n) ?
Confirm with 'y'. The bridge will save and restart with the new
settings.
```

6. Após a reinicialização da ponte FC-para-SAS, efetue login novamente.
7. Defina a velocidade nas portas FC usando o `set fcdatarate port speed` comando.
   - `port` pode ser "1" ou "2".
   - `speed` Pode ser "2 GB", "4 GB", "8 GB" ou "16 GB", dependendo da ponte do modelo.

   No exemplo a seguir, a velocidade da porta FC1 é definida como "8 GB".

```
Ready.
set fcdatarate 1 8Gb

Ready. *
```

8. Defina a topologia nas portas FC usando o `set FCConnMode port mode` comando.
   - `port` pode ser "1" ou "2".
   - `mode` pode ser "ptp", "loop", "ptp-loop" ou "auto".

   No exemplo a seguir, a topologia da porta FC1 é definida como "ptp".

```
Ready.
set FCConnMode 1 ptp

Ready. *
```

9. Salve a configuração usando o `saveConfiguration` comando e reinicie a ponte quando solicitado a fazê-lo.

   O exemplo a seguir mostra o `saveConfiguration` comando e o prompt para reiniciar a ponte.

```
 Ready.
 SaveConfiguration
    Restart is necessary....
    Do you wish to restart (y/n) ?
 Confirm with 'y'. The bridge will save and restart with the new
settings.
```

10. Após a reinicialização da ponte FC-para-SAS, efetue login novamente.
11. Se a ponte FC para SAS estiver executando o firmware 1,60 ou posterior, ative o SNMP.

```
Ready.
set snmp enabled

Ready. *
saveconfiguration

Restart is necessary....
Do you wish to restart (y/n) ?

Verify with 'y' to restart the FibreBridge.
```

12. Desligue as pontes FC para SAS.

Configuração dos switches FC (somente configurações MetroCluster FC)

Se você tiver substituído os switches FC no local de desastre, será necessário configurá-los usando os procedimentos específicos do fornecedor. Você deve configurar um switch, verificar se o acesso ao armazenamento no site sobrevivente não é afetado e, em seguida, configurar o segundo switch.

Tarefas relacionadas

"Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Configuração de um switch Brocade FC após um desastre no local

Deve utilizar este procedimento específico do Brocade para configurar o comutador de substituição e ativar as portas ISL.

Sobre esta tarefa

Os exemplos deste procedimento baseiam-se nas seguintes premissas:

- O local A é o local do desastre.
- FC_switch_A_1 foi substituído.
- FC_switch_A_2 foi substituído.
- O local B é o local sobrevivente.

- FC_switch_B_1 está em bom estado.
- FC_switch_B_2 está em bom estado.

Você deve verificar se está usando as atribuições de portas especificadas quando você faz o cabo dos switches FC:

- "Atribuições de portas para switches FC ao usar o ONTAP 9.1 e posterior"

Os exemplos mostram duas pontes FC-para-SAS. Se tiver mais bridges, tem de desativar e, posteriormente, ativar as portas adicionais.

Passos

1. Arranque e pré-configure o novo interrutor:

   a. Ligue o novo interrutor e deixe-o arrancar.

   b. Verifique a versão do firmware no switch para confirmar que corresponde à versão dos outros switches FC:

      `firmwareShow`

   c. Configure o novo switch conforme descrito nos tópicos a seguir, ignorando as etapas para configurar o zoneamento no switch.

      "Instalação e configuração do MetroCluster conectado à malha"

      "Instalação e configuração do Stretch MetroCluster"

   d. Desative o interrutor persistentemente:

      `switchcfgpersistentdisable`

      O switch permanecerá desativado após uma reinicialização ou fastboot. Se este comando não estiver disponível, você deve usar o `switchdisable` comando.

      O exemplo a seguir mostra o comando no BrocadeSwitchA:

      ```
      BrocadeSwitchA:admin> switchcfgpersistentdisable
      ```

      O exemplo a seguir mostra o comando no BrocadeSwitchB:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

2. Configuração completa do novo switch:

   a. Ative as ISLs no site sobrevivente:

      `portcfgpersistentenable port-number`

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

b. Ative as ISLs nos interrutores de substituição:

`portcfgpersistentenable port-number`

```
FC_switch_A_1:admin> portcfgpersistentenable 10
FC_switch_A_1:admin> portcfgpersistentenable 11
```

c. No interrutor de substituição (FC_switch_A_1 neste exemplo) verifique se os ISL estão online:

`switchshow`

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1" (downstream)
...
```

3. Ativar persistentemente o interrutor:

`switchcfgpersistentenable`

4. Verifique se as portas estão online:

`switchshow`

Configuração de um switch Cisco FC após um desastre no local

Você deve usar o procedimento específico do Cisco para configurar o switch de substituição e ativar as portas ISL.

Sobre esta tarefa

Os exemplos deste procedimento baseiam-se nas seguintes premissas:

- O local A é o local do desastre.
- FC_switch_A_1 foi substituído.
- FC_switch_A_2 foi substituído.
- O local B é o local sobrevivente.
- FC_switch_B_1 está em bom estado.
- FC_switch_B_2 está em bom estado.

Passos

1. Configure o interrutor:
   a. Consulte "Instalação e configuração do MetroCluster conectado à malha"
   b. Siga as etapas para configurar o switch "Configuração dos switches Cisco FC"na seção *excepto* para a seção "Configurando zoneamento em um switch Cisco FC":

      O zoneamento é configurado posteriormente neste procedimento.

2. No interrutor de integridade (neste exemplo, FC_switch_B_1), ative as portas ISL.

   O exemplo a seguir mostra os comandos para ativar as portas:

   ```
   FC_switch_B_1# conf t
   FC_switch_B_1(config)# int fc1/14-15
   FC_switch_B_1(config)# no shut
   FC_switch_B_1(config)# end
   FC_switch_B_1# copy running-config startup-config
   FC_switch_B_1#
   ```

3. Verifique se as portas ISL estão ativas usando o comando show interface brief.
4. Recupere as informações de zoneamento do tecido.

   O exemplo a seguir mostra os comandos para distribuir a configuração de zoneamento:

   ```
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 10
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 20
   FC_switch_B_1(config-zone)# end
   ```

   FC_switch_B_1 é distribuído para todos os outros switches na malha para "vsan 10" e "vsan 20", e as informações de zoneamento são recuperadas de FC_switch_A_1.

5. No interrutor de integridade, verifique se as informações de zoneamento estão corretamente recuperadas do switch de parceiro:

   `show zone`

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

6. Determine os nomes mundiais (WWNs) dos switches na malha do switch.

   Neste exemplo, as duas WWNs de switch são as seguintes:

   - FC_switch_A_1: 20:00:54:7f:EE:B8:24:C0
   - FC_switch_B_1: 20:00:54:7f:EE:C6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

7. Entre no modo de configuração para a zona e remova os membros da zona que não pertencem ao switch WWNs dos dois switches:

   `no member interface interface-ide swwn wwn`

   Neste exemplo, os seguintes membros não estão associados à WWN de nenhum dos switches na malha e devem ser removidos:

   - Nome da zona FC-VI_Zone_1_10 vsan 10
     - A interface FC1/1 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/2 oscila 20:00:54:7f:EE:e3:86:50

     > Os sistemas AFF A700 e FAS9000 são compatíveis com quatro portas FC-VI. É necessário remover todas as quatro portas da zona FC-VI.

   - Nome de zona STOR_Zone_1_20_25A vsan 20
     - A interface FC1/5 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/8 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/9 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/10 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/11 oscila 20:00:54:7f:EE:e3:86:50
   - Nome de zona STOR_Zone_1_20_25B vsan 20
     - A interface FC1/8 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/9 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/10 oscila 20:00:54:7f:EE:e3:86:50
     - A interface FC1/11 oscila 20:00:54:7f:EE:e3:86:50

   O exemplo a seguir mostra a remoção dessas interfaces:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

8. Adicione as portas do novo switch às zonas.

   O exemplo a seguir pressupõe que o cabeamento no switch de substituição é o mesmo que no switch antigo:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

9. Verifique se o zoneamento está configurado corretamente: `show zone`

   A saída de exemplo a seguir mostra as três zonas:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

Verificando a configuração do armazenamento

Você precisa confirmar se todo o storage está visível nos nós sobreviventes.

Passos

1. Confirme se todos os componentes de storage no local de desastre são os mesmos em quantidade e tipo no local sobrevivente.

   O local sobrevivente e o local de desastre devem ter o mesmo número de stacks de gaveta de disco, gavetas de disco e discos. Em uma configuração MetroCluster conectada a uma ponte ou conetada a malha, os locais devem ter o mesmo número de pontes FC para SAS.

2. Confirme se todos os discos que foram substituídos no local de desastre não são de propriedade:

   `run local disk show-n`

   Os discos devem aparecer como sendo não possuídos.

3. Se nenhum disco tiver sido substituído, confirme se todos os discos estão presentes:

   ```
   disk show
   ```

Ligar o equipamento no local de desastre

Você precisa ligar os componentes do MetroCluster no local de desastre quando estiver pronto para se preparar para o switchback. Além disso, você também precisa reabilitar as conexões de armazenamento SAS em configurações MetroCluster de conexão direta e habilitar portas de conexão não inter-switch em configurações MetroCluster conetadas à malha.

Antes de começar

Você já deve ter substituído e cabeado os componentes do MetroCluster exatamente como os antigos.

"Instalação e configuração do MetroCluster conectado à malha"

"Instalação e configuração do Stretch MetroCluster"

Sobre esta tarefa

Os exemplos deste procedimento assumem o seguinte:

- O local A é o local do desastre.
  - FC_switch_A_1 foi substituído.
  - FC_switch_A_2 foi substituído.
- O local B é o local sobrevivente.
  - FC_switch_B_1 está em bom estado.
  - FC_switch_B_2 está em bom estado.

Os switches FC estão presentes apenas nas configurações MetroCluster conectadas à malha.

Passos

1. Em uma configuração MetroCluster estendida usando cabeamento SAS (e sem malha de switch FC ou pontes FC para SAS), conecte todo o storage, incluindo o storage remoto, em ambos os locais.

   O controlador no local de desastre deve permanecer desligado ou no prompt DO Loader.

2. No site sobrevivente, desative a atribuição automática do disco:

   ```
   storage disk option modify -autoassign off *
   ```

   ```
   cluster_B::> storage disk option modify -autoassign off *
   2 entries were modified.
   ```

3. No site sobrevivente, confirme se a atribuição automática do disco está desativada:

   ```
   storage disk option show
   ```

```
cluster_B::> storage disk option show
Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          off             default
node_B_2       on            on          off             default
2 entries were displayed.

 cluster_B::>
```

4. Ligue as gavetas de disco no local de desastre e verifique se todos os discos estão em execução.
5. Em uma configuração MetroCluster conectada a uma ponte ou conetada a malha, ative todas as pontes FC para SAS no local do desastre.
6. Se algum disco tiver sido substituído, deixe os controladores desligados ou no prompt DO Loader.
7. Em uma configuração MetroCluster conetada à malha, habilite as portas não ISL nos switches FC.

Se o fornecedor do switch for…	Em seguida, utilize estes passos para ativar as portas…

Brocade	a. Habilite persistentemente as portas conetadas às bridges FC-para-SAS: `portpersistentenable port-number` No exemplo a seguir, as portas 6 e 7 estão ativadas: ``` FC_switch_A_1:admin>portpersistentenable 6 FC_switch_A_1:admin>portpersistentenable 7 FC_switch_A_1:admin> ``` b. Habilite persistentemente as portas conetadas aos HBAs e adaptadores FC-VI: `portpersistentenable port-number` No exemplo a seguir, as portas 6 e 7 estão ativadas: ``` FC_switch_A_1:admin>portpersistentenable 1 FC_switch_A_1:admin>portpersistentenable 2 FC_switch_A_1:admin>portpersistentenable 4 FC_switch_A_1:admin>portpersistentenable 5 FC_switch_A_1:admin> ``` Para sistemas AFF A700 e FAS9000, você deve ativar persistentemente todas as quatro portas FC-VI usando o comando switchcfgpersistentemente. c. Repita os subpassos a e b para o segundo switch FC no local sobrevivente.

Cisco	a. Entre no modo de configuração para a interface e, em seguida, ative as portas com o comando no shut. No exemplo a seguir, a porta FC1/36 está desativada: `FC_switch_A_1# conf t` `FC_switch_A_1(config)# interface fc1/36` `FC_switch_A_1(config)# no shut` `FC_switch_A_1(config-if)# end` `FC_switch_A_1# copy running-config startup-config` b. Verifique se a porta do switch está ativada: `show interface brief` c. Repita as subetapas a e b nas outras portas conectadas às pontes FC-para-SAS, HBAs e adaptadores FC-VI. d. Repita os subpassos a, b e c para o segundo switch FC no local sobrevivente.

Atribuição de propriedade para unidades substituídas

Se você substituiu unidades ao restaurar o hardware no local de desastre ou se você tivesse que zero unidades ou remover a propriedade, você deverá atribuir propriedade às unidades afetadas.

Antes de começar

O local de desastre deve ter pelo menos quantas unidades disponíveis antes do desastre.

O arranjo de compartimentos e unidades de unidades deve atender aos requisitos "Componente IP do MetroCluster necessário e convenções de nomenclatura" da "Instalação e configuração IP do MetroCluster"seção do .

Sobre esta tarefa

Essas etapas são executadas no cluster no local do desastre.

Este procedimento mostra a reatribuição de todas as unidades e a criação de novos plexos no local de desastre. Os novos plexos são plexos remotos do local sobrevivente e dos plexos locais do local do desastre.

Esta seção fornece exemplos para configurações de dois e quatro nós. Para configurações de dois nós, você pode ignorar referências ao segundo nó em cada local. Para configurações de oito nós, você deve ter em conta os nós adicionais no segundo grupo de DR. Os exemplos fazem as seguintes suposições:

- O local A é o local do desastre.

    - O nó_A_1 foi substituído.
    - O nó_A_2 foi substituído.

      Presente apenas em configurações de MetroCluster de quatro nós.

- O local B é o local sobrevivente.
    - Node_B_1 está em bom estado.
    - Node_B_2 está em bom estado.

      Presente apenas em configurações de MetroCluster de quatro nós.

Os módulos do controlador têm as seguintes IDs de sistema originais:

Número de nós na configuração do MetroCluster	Nó	ID do sistema original
Quatro	node_A_1	4068741258
node_A_2	4068741260	node_B_1
4068741254	node_B_2	4068741256
Dois	node_A_1	4068741258

Você deve ter em mente os seguintes pontos ao atribuir as unidades:

- A contagem antiga de discos deve ter pelo menos o mesmo número de discos para cada nó que estava presente antes do desastre.

  Se um número menor de discos for especificado ou presente, as operações de recuperação podem não ser concluídas devido a espaço insuficiente.

- Os novos plexos a serem criados são plexos remotos pertencentes ao local sobrevivente (node_B_x pool1) e plexos locais pertencentes ao local de desastre (node_B_x pool0).
- O número total de unidades necessárias não deve incluir os discos raiz aggrr.

  Se n discos forem atribuídos a pool1 do local sobrevivente, os discos n-3 devem ser atribuídos ao local de desastre com a suposição de que o agregado raiz usa três discos.

- Nenhum dos discos pode ser atribuído a um pool que é diferente daquele ao qual todos os outros discos na mesma pilha são atribuídos.
- Os discos pertencentes ao local sobrevivente são atribuídos ao pool 1 e os discos pertencentes ao local de desastre são atribuídos ao pool 0.

Passos

1. Atribua as novas unidades sem propriedade com base se você tem uma configuração de MetroCluster de quatro nós ou dois nós:

    - Para configurações de MetroCluster de quatro nós, atribua os novos discos não possuídos aos pools de discos apropriados usando a seguinte série de comandos nos nós de substituição:

i. Atribua sistematicamente os discos substituídos para cada nó aos respetivos pools de discos:

```
disk assign -s sysid -n old-count-of-disks -p pool
```

No site sobrevivente, você emite um comando de atribuição de disco para cada nó:

```
cluster_B::> disk assign -s node_B_1-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_B_2-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_A_1-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
cluster_B::> disk assign -s node_A_2-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
```

O exemplo a seguir mostra os comandos com as IDs do sistema:

```
cluster_B::> disk assign -s 4068741254 -n 21 -p 1
cluster_B::> disk assign -s 4068741256 -n 21 -p 1
cluster_B::> disk assign -s 4068741258 -n 21 -p 0
cluster_B::> disk assign -s 4068741260 -n 21 -p 0
```

i. Confirme a propriedade dos discos:

```
storage disk show -fields owner, pool
```

```
storage disk show -fields owner, pool
cluster_A::> storage disk show -fields owner, pool
disk     owner          pool
-------- ------------- -----
0c.00.1  node_A_1      Pool0
0c.00.2  node_A_1      Pool0
.
.
.
0c.00.8  node_A_1      Pool1
0c.00.9  node_A_1      Pool1
.
.
.
0c.00.15 node_A_2      Pool0
0c.00.16 node_A_2      Pool0
.
.
.
0c.00.22 node_A_2      Pool1
0c.00.23 node_A_2      Pool1
.
.
.
```

- Para configurações de MetroCluster de dois nós, atribua os novos discos não possuídos aos pools de discos apropriados usando a seguinte série de comandos no nó de substituição:
  i. Exibir as IDs de gaveta locais:

     ```
     run local storage show shelf
     ```

  ii. Atribua os discos substituídos para o nó íntegro ao pool 1:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 1 -s
     node_B_1-sysid -f
     ```

  iii. Atribua os discos substituídos para o nó de substituição ao pool 0:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 0 -s
     node_A_1-sysid -f
     ```

2. No site sobrevivente, ative novamente a atribuição automática de disco:

```
storage disk option modify -autoassign on *
```

```
cluster_B::> storage disk option modify -autoassign on *
2 entries were modified.
```

3. No site sobrevivente, confirme se a atribuição automática de disco está em:

   `storage disk option show`

```
 cluster_B::> storage disk option show
 Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          on              default
node_B_2       on            on          on              default
2 entries were displayed.

 cluster_B::>
```

Informações relacionadas

"Gerenciamento de disco e agregado"

"Como as configurações do MetroCluster usam o SyncMirror para fornecer redundância de dados"

Executando recuperação de agregados e restauração de espelhos (configurações MetroCluster FC)

Depois de substituir o hardware e atribuir discos, você pode executar as operações de recuperação do MetroCluster. Em seguida, você deve confirmar se os agregados estão espelhados e, se necessário, reiniciar o espelhamento.

Passos

1. Execute as duas fases de cura (cura agregada e recuperação de raiz) no local de desastre:

```
cluster_B::> metrocluster heal -phase aggregates

cluster_B::> metrocluster heal -phase root-aggregates
```

2. Monitore a recuperação e verifique se os agregados estão no estado ressincronizado ou espelhado:

   `storage aggregate show -node local`

Se o agregado mostrar este estado…	Então…
ressincronização	Nenhuma ação é necessária. Deixe o agregado concluir a ressincronização.

espelho degradado	Prossiga para Se um ou mais plexes permanecerem offline, etapas adicionais serão necessárias para reconstruir o espelho.
espelhado, normal	Nenhuma ação é necessária.
desconhecido, offline	O agregado raiz mostra esse estado se todos os discos nos locais de desastre foram substituídos.

```
cluster_B::> storage aggregate show -node local

 Aggregate     Size Available Used% State   #Vols  Nodes      RAID
Status
 --------- -------- --------- ----- ------- ------ ----------
------------
 node_B_1_aggr1
            227.1GB   11.00GB   95% online       1 node_B_1   raid_dp,
                                                              resyncing
 NodeA_1_aggr2
            430.3GB   28.02GB   93% online       2 node_B_1   raid_dp,
                                                              mirror
                                                              degraded
 node_B_1_aggr3
            812.8GB   85.37GB   89% online       5 node_B_1   raid_dp,
                                                              mirrored,
                                                              normal
 3 entries were displayed.

cluster_B::>
```

Nos exemplos a seguir, os três agregados estão cada um em um estado diferente:

Nó	Estado
node_B_1_aggr1	ressincronização
node_B_1_aggr2	espelho degradado
node_B_1_aggr3	espelhado, normal

3. se um ou mais plexes permanecerem off-line, etapas adicionais serão necessárias para reconstruir o espelho.

   Na tabela anterior, o espelho para node_B_1_aggr2 deve ser reconstruído.

a. Veja os detalhes do agregado para identificar quaisquer plexos com falha:

```
storage aggregate show -r -aggregate node_B_1_aggr2
```

No exemplo a seguir, Plex /node_B_1_aggr2/plex0 está em um estado com falha:

```
cluster_B::> storage aggregate show -r -aggregate node_B_1_aggr2

 Owner Node: node_B_1
  Aggregate: node_B_1_aggr2 (online, raid_dp, mirror degraded) (block
checksums)
   Plex: /node_B_1_aggr2/plex0 (offline, failed, inactive, pool0)
    RAID Group /node_B_1_aggr2/plex0/rg0 (partial)
                                                                    Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------

   Plex: /node_B_1_aggr2/plex1 (online, normal, active, pool1)
    RAID Group /node_B_1_aggr2/plex1/rg0 (normal, block checksums)
                                                                    Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------
      dparity  1.44.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      parity   1.41.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.42.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.44.9                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.18                   1   SAS    15000  265.6GB
273.5GB (normal)
 6 entries were displayed.

 cluster_B::>
```

a. Eliminar o Plex com falha:

```
storage aggregate plex delete -aggregate aggregate-name -plex plex
```

b. Restabelecer o espelho:

```
storage aggregate mirror -aggregate aggregate-name
```

c. Monitore o status de ressincronização e espelhamento do Plex até que todos os espelhos sejam restabelecidos e todos os agregados mostrem espelhado status normal:

```
storage aggregate show
```

Reatribuir a propriedade do disco para agregados raiz a módulos de controladora de substituição (configurações MetroCluster FC)

Se um ou ambos os módulos da controladora ou placas NVRAM tiverem sido substituídos no local de desastre, o ID do sistema foi alterado e você deve reatribuir discos pertencentes aos agregados raiz aos módulos da controladora de substituição.

Sobre esta tarefa

Como os nós estão no modo de switchover e a recuperação foi feita, apenas os discos que contêm os agregados raiz de pool1 do local de desastre serão reatribuídos nesta seção. Eles são os únicos discos ainda possuídos pelo ID do sistema antigo neste momento.

Esta seção fornece exemplos para configurações de dois e quatro nós. Para configurações de dois nós, você pode ignorar referências ao segundo nó em cada local. Para configurações de oito nós, você deve ter em conta os nós adicionais no segundo grupo de DR. Os exemplos fazem as seguintes suposições:

- O local A é o local do desastre.
  - O nó_A_1 foi substituído.
  - O nó_A_2 foi substituído.

    Presente apenas em configurações de MetroCluster de quatro nós.
- O local B é o local sobrevivente.
  - Node_B_1 está em bom estado.
  - Node_B_2 está em bom estado.

    Presente apenas em configurações de MetroCluster de quatro nós.

Os IDs de sistema antigo e novo foram identificados no "Substitua o hardware e inicialize novos controladores".

Os exemplos neste procedimento usam controladores com as seguintes IDs de sistema:

Número de nós	Nó	ID do sistema original	Nova ID do sistema

Quatro	node_A_1	4068741258	1574774970
	node_A_2	4068741260	1574774991
	node_B_1	4068741254	inalterado
	node_B_2	4068741256	inalterado
Dois	node_A_1	4068741258	1574774970

Passos

1. Com o nó de substituição no modo Manutenção, reatribua os discos agregados raiz:

   `disk reassign -s old-system-ID -d new-system-ID`

   ```
   *> disk reassign -s 4068741258 -d 1574774970
   ```

2. Visualize os discos para confirmar a alteração de propriedade dos discos de pool1 raiz aggr do local de desastre para o nó de substituição:

   `disk show`

   A saída pode mostrar mais ou menos discos, dependendo de quantos discos estão no agregado raiz e se algum desses discos falhou e foi substituído. Se os discos foram substituídos, então Pool0 discos não aparecerão na saída.

   Os discos agregados de raiz pool1 do local de desastre agora devem ser atribuídos ao nó de substituição.

```
*> disk show
Local System ID: 1574774970

  DISK             OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------       -------------         -----  -------------
-------------       -------------
sw_A_1:6.126L19    node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L3     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L7     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_B_1:6.126L8     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L24    node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L2     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)

*> aggr status
         Aggr State           Status
 node_A_1_root online          raid_dp, aggr
                               mirror degraded
                               64-bit
*>
```

3. Exibir o status agregado:

   `aggr status`

   A saída pode mostrar mais ou menos discos, dependendo de quantos discos estão no agregado raiz e se algum desses discos falhou e foi substituído. Se os discos tiverem sido substituídos, os discos Pool0 não aparecerão na saída.

```
*> aggr status
          Aggr State           Status
  node_A_1_root online          raid_dp, aggr
                                mirror degraded
                                64-bit
*>
```

4. Elimine o conteúdo dos discos da caixa de correio:

   `mailbox destroy local`

5. Se o agregado não estiver online, coloque-o online:

   ```
   aggr online aggr_name
   ```

6. Interrompa o nó para exibir o prompt DO Loader:

   ```
   halt
   ```

Iniciar os novos módulos de controladores (configurações MetroCluster FC)

Após a conclusão da recuperação de agregado para os agregados de dados e raiz, você precisa inicializar o nó ou nós no local de desastre.

Sobre esta tarefa

Esta tarefa começa com os nós mostrando o prompt Loader.

Passos

1. Apresentar o menu de arranque:

   ```
   boot_ontap menu
   ```

2. a partir do menu de arranque, selecione a opção 6, **Atualizar flash a partir da configuração de cópia de segurança**.
3. Responda `y` ao seguinte aviso:

   ```
   This will replace all flash-based configuration with the last backup to disks.
   Are you sure you want to continue?: y
   ```

   O sistema será inicializado duas vezes, a segunda vez para carregar a nova configuração.

   > Se você não limpar o conteúdo do NVRAM de um controlador de substituição usado, poderá ver um pânico com a seguinte mensagem: `PANIC: NVRAM contents are invalid...` Se isso ocorrer, repita No menu de inicialização, selecione a opção 6, **Atualizar flash a partir da configuração de backup**. para inicializar o sistema no prompt do ONTAP. Então você precisa Redefina a recuperação de inicialização e os bootargs rdb_corrupt

4. Espelhar o agregado de raiz no Plex 0:
   a. Atribua três discos pool0 ao novo módulo do controlador.
   b. Espelhar o agregado de raiz pool1 Plex:

      ```
      aggr mirror root-aggr-name
      ```

   c. Atribua discos não possuídos a pool0 no nó local
5. Se você tiver uma configuração de quatro nós, repita as etapas anteriores no outro nó no local de desastre.
6. Atualize a configuração do MetroCluster:
   a. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

b. Atualizar a configuração:

```
metrocluster configure -refresh true
```

c. Voltar ao modo de privilégios de administrador:

```
set -privilege admin
```

7. Confirme se os nós de substituição no local de desastre estão prontos para o switchback:

```
metrocluster node show
```

Os nós de substituição devem estar no modo "'aguardando a recuperação de switchback'". Se eles estiverem no modo "normal", você pode reinicializar os nós de substituição. Após essa inicialização, os nós devem estar no modo "'aguardando a recuperação de switchback".

O exemplo a seguir mostra que os nós de substituição estão prontos para switchback:

```
cluster_B::> metrocluster node show
DR                    Configuration  DR
Grp Cluster Node      State          Mirroring Mode
--- ------- --------- -------------- --------- --------------------
1   cluster_B
            node_B_1  configured     enabled   switchover completed
            node_B_2  configured     enabled   switchover completed
    cluster_A
            node_A_1  configured     enabled   waiting for switchback
recovery
            node_A_2  configured     enabled   waiting for switchback
recovery
4 entries were displayed.

cluster_B::>
```

O que fazer a seguir

Prossiga para "Conclua o processo de recuperação de desastres".

Reponha os bootargs boot_recovery e rdb_corrupt

Se necessário, você pode redefinir o boot_recovery e o rdb_corrupt_bootargs

Passos

1. Interrompa o nó de volta ao prompt DO Loader:

```
node_A_1::*> halt -node _node-name_
```

2. Verifique se os seguintes bootargs foram definidos:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se qualquer bootarg tiver sido definido como um valor, desconfigure-o e inicie o ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Preparando-se para switchback em uma configuração mista (recuperação durante a transição)

É necessário executar determinadas tarefas para preparar a configuração mista de IP e FC do MetroCluster para a operação de switchback. Este procedimento aplica-se apenas a configurações que encontraram uma falha durante o processo de transição MetroCluster FC para IP.

Sobre esta tarefa

Este procedimento só deve ser usado quando se executa a recuperação em um sistema que estava em transição intermediária quando ocorreu a falha.

Nesse cenário, o MetroCluster é uma configuração mista:

- Um grupo de DR consiste em nós FC da MetroCluster conectados a malha.

  Você deve executar as etapas de recuperação do MetroCluster FC nesses nós.

- Um grupo de DR consiste em nós IP do MetroCluster.

  Você deve executar as etapas de recuperação do IP do MetroCluster nesses nós.

Passos

Execute as etapas na ordem a seguir.

1. Prepare os nós FC para o switchback executando as seguintes tarefas em ordem:
   a. "Verificação da configuração da porta (somente configurações MetroCluster FC)"
   b. "Configuração de pontes FC para SAS (somente configurações de MetroCluster FC)"
   c. "Configuração dos switches FC (somente configurações MetroCluster FC)"
   d. "Verificando a configuração do armazenamento" (Execute apenas estas etapas em unidades substituídas nos nós FC do MetroCluster)
   e. "Ligar o equipamento no local de desastre" (Execute apenas estas etapas em unidades substituídas nos nós FC do MetroCluster)

f. "Atribuição de propriedade para unidades substituídas" (Execute apenas estas etapas em unidades substituídas nos nós FC do MetroCluster)

g. Execute as etapas em "Reatribuir a propriedade do disco para agregados raiz a módulos de controladora de substituição (configurações MetroCluster FC)", até e incluindo a etapa para emitir o comando Mailbox Destroy.

h. Destrua o Plex local (Plex 0) do agregado raiz:

```
aggr destroy plex-id
```

i. Se o aggr raiz não estiver online, coloque-o online.

2. Inicialize os nós de MetroCluster FC.

Siga estas etapas em ambos os nós do MetroCluster FC.

a. Apresentar o menu de arranque:

```
boot_ontap menu
```

b. No menu de inicialização, selecione a opção 6, **Atualizar flash a partir da configuração de backup**.

c. Responda `y` ao seguinte aviso:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?: y
```

O sistema será inicializado duas vezes, a segunda vez para carregar a nova configuração.

> Se você não limpar o conteúdo do NVRAM de um controlador de substituição usado, poderá ver um pânico com a seguinte mensagem: `PANIC: NVRAM contents are invalid...` Se isso ocorrer, repita estas subetapas para inicializar o sistema no prompt do ONTAP. Então você precisa Redefina a recuperação de inicialização e os bootargs rdb_corrupt

3. Espelhar o agregado de raiz no Plex 0:

Siga estas etapas em ambos os nós do MetroCluster FC.

a. Atribua três discos pool0 ao novo módulo do controlador.

b. Espelhar o agregado de raiz pool1 Plex:

```
aggr mirror root-aggr-name
```

c. Atribua discos não possuídos a pool0 no nó local

4. Regressar ao modo de manutenção.

Siga estas etapas em ambos os nós do MetroCluster FC.

a. Parar o nó:

```
halt
```

b. Inicialize o nó para Manutenção:

```
mode:boot_ontap maint
```

5. Elimine o conteúdo dos discos da caixa de correio:

   ```
   mailbox destroy local
   ```

   Siga estas etapas em ambos os nós do MetroCluster FC.

6. Parar os nós: Mais
   `halt`
7. Após a inicialização dos nós, verifique o status do nó:

   ```
   metrocluster node show
   ```

   ```
   siteA::*> metrocluster node show
   DR                               Configuration  DR
   Group Cluster Node               State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     siteA
                 wmc66-a1           configured     enabled   waiting for
   switchback recovery
                 wmc66-a2           configured     enabled   waiting for
   switchback recovery
         siteB
                 wmc66-b1           configured     enabled   switchover
   completed
                 wmc66-b2           configured     enabled   switchover
   completed
   2     siteA
                 wmc55-a1           -              -         -
                 wmc55-a2           unreachable    -         -
         siteB
                 wmc55-b1           configured     enabled   switchover
   completed
                 wmc55-b2           configured
   ```

8. Prepare os nós IP do MetroCluster para o switchback executando as tarefas em "Preparando-se para switchback em uma configuração IP MetroCluster" até e incluindo "Exclusão de plexes com falha de propriedade do site sobrevivente (configurações IP do MetroCluster)".
9. Nos nós de FC do MetroCluster, execute as etapas em "Executando recuperação de agregados e restauração de espelhos (configurações MetroCluster FC)".
10. Nos nós IP do MetroCluster, execute as etapas em "Executar a recuperação de agregados e restaurar espelhos (configurações IP do MetroCluster)".
11. Prossiga pelas tarefas restantes do processo de recuperação, começando com "Restabelecimento de armazenamentos de objetos para configurações do FabricPool".

Reponha os bootargs boot_recovery e rdb_corrupt

Se necessário, você pode redefinir o boot_recovery e o rdb_corrupt_bootargs

Passos

1. Interrompa o nó de volta ao prompt DO Loader:

```
node_A_1::*> halt -node _node-name_
```

2. Verifique se os seguintes bootargs foram definidos:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se qualquer bootarg tiver sido definido como um valor, desconfigure-o e inicie o ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

A concluir a recuperação

Execute as tarefas necessárias para concluir a recuperação de uma falha de vários controladores ou armazenamento.

Restabelecimento de armazenamentos de objetos para configurações do FabricPool

Se um dos armazenamentos de objetos em um espelho do FabricPool foi co-localizado com o local de desastre do MetroCluster e foi destruído, você deve restabelecer o armazenamento de objetos e o espelho do FabricPool.

Sobre esta tarefa

- Se os armazenamentos de objetos forem remotos e um site MetroCluster for destruído, você não precisará reconstruir o armazenamento de objetos e as configurações originais do armazenamento de objetos, bem como o conteúdo de dados inativos serão retidos.
- Para obter mais informações sobre configurações do FabricPool, consulte "Gerenciamento de disco e agregados".

Passo

1. Seguir o procedimento "Substituição de um espelho FabricPool numa configuração MetroCluster" no "Gerenciamento de disco e agregados".

Verificando licenças nos nós substituídos

Você deve instalar novas licenças para os nós de substituição se os nós deficientes estiverem usando

recursos do ONTAP que exigem uma licença padrão (node-locked). Para recursos com licenças padrão, cada nó no cluster deve ter sua própria chave para o recurso.

Sobre esta tarefa

Até instalar chaves de licença, os recursos que exigem licenças padrão continuam disponíveis para o nó de substituição. No entanto, se o nó prejudicado for o único nó no cluster com uma licença para o recurso, nenhuma alteração de configuração será permitida. Além disso, o uso de recursos não licenciados no nó pode deixá-lo fora de conformidade com o contrato de licença, portanto, você deve instalar a chave de licença de substituição ou as chaves no nó de substituição o mais rápido possível.

As chaves de licença devem estar no formato de 28 carateres.

Você tem um período de carência de 90 dias para instalar as chaves de licença. Após o período de carência, todas as licenças antigas são invalidadas. Depois que uma chave de licença válida é instalada, você tem 24 horas para instalar todas as chaves antes que o período de carência termine.

Se todos os nós de um local tiverem sido substituídos (um único nó no caso de uma configuração de MetroCluster de dois nós), as chaves de licença devem ser instaladas no nó ou nós de substituição antes do switchback.

Passos

1. Identifique as licenças no nó:

   ```
   license show
   ```

   O exemplo a seguir exibe as informações sobre licenças no sistema:

   ```
   cluster_B::>  license show
            (system license show)

   Serial Number: 1-80-00050
   Owner: site1-01
   Package           Type       Description             Expiration
   -------           -------    -------------           -----------
   Base              license    Cluster Base License        -
   NFS               site       NFS License                 -
   CIFS              site       CIFS License                -
   iSCSI             site       iSCSI License               -
   FCP               site       FCP License                 -
   FlexClone         site       FlexClone License           -

   6 entries were displayed.
   ```

2. Verifique se as licenças são boas para o nó após o switchback:

   ```
   metrocluster check license show
   ```

   O exemplo a seguir exibe as licenças que são boas para o nó:

```
cluster_B::> metrocluster check license show

Cluster           Check                              Result
-------           -------                            -------------
Cluster_B         negotiated-switchover-ready        not-applicable
NFS               switchback-ready                   not-applicable
CIFS              job-schedules                      ok
iSCSI             licenses                           ok
FCP               periodic-check-enabled             ok
```

3. Se você precisar de novas chaves de licença, obtenha chaves de licença de substituição no site de suporte da NetApp na seção meu suporte em licenças de software.

> As novas chaves de licença que você precisa são geradas automaticamente e enviadas para o endereço de e-mail em arquivo. Se não receber o e-mail com as chaves de licença no prazo de 30 dias, consulte a secção *"Quem contactar se tiver problemas com as minhas licenças?"* no artigo da base de dados de Conhecimento "Pós-processo de substituição da placa-mãe para atualizar o licenciamento em um sistema AFF/FAS."

4. Instale cada chave de licença:

```
system license add -license-code license-key, license-key…+
```

5. Remova as licenças antigas, se desejar:
   a. Verifique se há licenças não utilizadas:

```
license clean-up -unused -simulate
```

   b. Se a lista estiver correta, remova as licenças não utilizadas:

```
license clean-up -unused
```

Restaurar o gerenciamento de chaves

Se os volumes de dados estiverem criptografados, você precisará restaurar o gerenciamento de chaves. Se o volume raiz estiver criptografado, você deverá recuperar o gerenciamento de chaves.

Passos

1. Se os volumes de dados estiverem criptografados, restaure as chaves usando o comando correto para a configuração de gerenciamento de chaves.

Se você estiver usando…	Use este comando…
Gestão de chaves a bordo	`security key-manager onboard sync` Para obter mais informações, "Restaurar chaves de criptografia integradas de gerenciamento de chaves"consulte .

Gerenciamento de chaves externas	`security key-manager key query -node node-name` Para obter mais informações, "Restaurar chaves de criptografia de gerenciamento de chaves externas"consulte .

2. Se o volume raiz estiver encriptado, utilize o procedimento em "Recuperar o gerenciamento de chaves se o volume raiz for criptografado".

Executando um switchback

Depois de curar a configuração do MetroCluster, você pode executar a operação MetroCluster switchback. A operação de switchback do MetroCluster retorna a configuração ao seu estado operacional normal, com as máquinas virtuais de armazenamento de origem sincronizada (SVMs) no local de desastre ativas e fornecendo dados dos pools de discos locais.

Antes de começar

- O cluster de desastres deve ter mudado com sucesso para o cluster sobrevivente.
- A recuperação deve ter sido realizada nos agregados de dados e raiz.
- Os nós de cluster sobreviventes não devem estar no estado de failover de HA (todos os nós precisam estar ativos e em execução para cada par de HA).
- Os módulos do controlador do local de desastre devem ser completamente inicializados e não no modo de aquisição de HA.
- O agregado raiz deve ser espelhado.
- Os links interswitches (ISLs) devem estar online.
- Todas as licenças necessárias devem ser instaladas no sistema.

Passos

1. Confirme se todos os nós estão no estado ativado:

   ```
   metrocluster node show
   ```

   O exemplo a seguir exibe os nós que estão no estado habilitado:

```
cluster_B::>  metrocluster node show

DR                        Configuration  DR
Group Cluster Node        State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Confirme se a ressincronização está concluída em todos os SVMs:

   `metrocluster vserver show`

3. Verifique se todas as migrações automáticas de LIF que estão sendo executadas pelas operações de recuperação foram concluídas com sucesso:

   `metrocluster check lif show`

4. Execute o switchback executando o `metrocluster switchback` comando de qualquer nó no cluster sobrevivente.
5. Verifique o progresso do funcionamento do interrutor de comutação:

   `metrocluster show`

   A operação de switchback ainda está em andamento quando a saída exibe "Waiting-for-switchback":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   A operação de comutação está concluída quando a saída exibe "normal":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o seguinte comando no nível avançado de privilégio:

```
metrocluster config-replication resync-status show
```

6. Restabelecer qualquer configuração SnapMirror ou SnapVault.

   No ONTAP 8,3, você precisa restabelecer manualmente uma configuração de SnapMirror perdida após uma operação de switchback MetroCluster. No ONTAP 9.0 e mais tarde, o relacionamento é restabelecido automaticamente.

Verificando um switchback bem-sucedido

Depois de executar o switchback, você deseja confirmar que todos os agregados e máquinas virtuais de storage (SVMs) são trocados de volta e on-line.

Passos

1. Verifique se os agregados de dados comutados estão invertidos:

   ```
   storage aggregate show
   ```

   No exemplo a seguir, aggr_B2 no nó B2 mudou de volta:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Se o local de desastre incluiu agregados sem espelhamento e os agregados sem espelhamento não estiverem mais presentes, o agregado pode aparecer com um estado de "'desconhecido'" na saída do comando storage Aggregate show. Para remover as entradas desatualizadas para os agregados sem espelhamento, consulte o artigo da base de dados de Conhecimento "Como remover entradas agregadas sem espelhamento obsoletas em um MetroCluster após desastre em que o armazenamento foi perdido."

2. Verifique se todos os SVMs de destino de sincronização no cluster sobrevivente estão inativos (mostrando um estado de administrador "coberto") e os SVMs de origem de sincronização no cluster de desastres estão ativos e em execução:

   ```
   vserver show -subtype sync-source
   ```

```
node_B_1::> vserver show -subtype sync-source
                                Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                                running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                                Admin      Root
Name    Name
Vserver             Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------         ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                       stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Os agregados de destino de sincronização na configuração do MetroCluster têm o sufixo "-mc" automaticamente anexado ao seu nome para ajudar a identificá-los.

3. Confirme se as operações de switchback foram bem-sucedidas usando o `metrocluster operation show` comando.

Se o comando output mostrar…	Então…
Que o estado de operação de comutação é bem-sucedido.	O processo de switchback está concluído e você pode prosseguir com a operação do sistema.
Que a operação de switchback ou switchback-continuation-Agent é parcialmente bem-sucedida.	Execute a correção sugerida fornecida na saída do comando MetroCluster operation show.

Depois de terminar

Você deve repetir as seções anteriores para executar o switchback na direção oposta. Se o site_A fez um switchover do site_B, faça um switchover do site_A.

Espelhando os agregados de raiz dos nós de substituição

Se os discos tiverem sido substituídos, você precisará espelhar os agregados raiz dos novos nós no local de desastre.

Passos

1. No local do desastre, identifique os agregados que não são espelhados:

   `storage aggregate show`

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1
raid4,

normal
node_A_2_aggr0
            1.49TB   74.12GB   95% online       1 node_A_2
raid4,

normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1         raid
4, normal

mirrored
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2         raid
4, normal

mirrored
4 entries were displayed.

cluster_A::>
```

2. Espelhar um dos agregados de raiz:

   `storage aggregate mirror -aggregate root-aggregate`

   O exemplo a seguir mostra como o comando seleciona discos e solicita confirmação ao espelhar o agregado.

```
cluster_A::> storage aggregate mirror -aggregate node_A_2_aggr0

Info: Disks would be added to aggregate "node_A_2_aggr0" on node
"node_A_2" in
      the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid4)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          parity     2.10.0                    SSD
-
          data       1.11.19                   SSD
894.0GB
          data       2.10.2                    SSD
894.0GB

      Aggregate capacity available for volume use would be 1.49TB.

Do you want to continue? {y|n}: y

cluster_A::>
```

3. Verifique se o espelhamento do agregado raiz está concluído:

   `storage aggregate show`

   O exemplo a seguir mostra que os agregados raiz são espelhados.

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr0
            2.24TB   838.5GB   63% online       1 node_A_2    raid4,
                                                               mirrored,
                                                               normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2    raid4
                                                               mirrored,
                                                               normal
4 entries were displayed.

cluster_A::>
```

4. Repita estas etapas para os outros agregados de raiz.

   Qualquer agregado de raiz que não tenha o status espelhado deve ser espelhado.

Reconfigurar o serviço do Mediador ONTAP (configurações IP do MetroCluster)

Se você tiver uma configuração IP do MetroCluster configurada com o serviço Mediador do ONTAP, remova e reconfigure a associação com o mediador.

Antes de começar

- Você deve ter o endereço IP, o nome de usuário e a senha para o serviço do Mediador ONTAP.
- O serviço Mediador ONTAP deve ser configurado e operar no host Linux.

Passos

1. Remova a configuração do Mediador ONTAP existente:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Reconfigure a configuração do Mediador ONTAP:

   ```
   metrocluster configuration-settings mediator add -mediator-address mediator-
   ```

```
IP-address
```

Verificando a integridade da configuração do MetroCluster

Você deve verificar a integridade da configuração do MetroCluster para verificar o funcionamento correto.

Passos

1. Verifique se o MetroCluster está configurado e no modo normal em cada cluster:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Verifique se o espelhamento está ativado em cada nó:

   ```
   metrocluster node show
   ```

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Verifique se os componentes do MetroCluster estão em bom estado:

   ```
   metrocluster check run
   ```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the `metrocluster check show -instance` command
or sub-commands in `metrocluster check` directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run `metrocluster switchover -simulate` or `metrocluster
switchback -simulate`, respectively.
```

4. Verifique se não existem alertas de saúde:

   `system health alert show`

5. Simular uma operação de comutação:

   a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado:

      `set -privilege advanced`

   Você precisa responder com `y` quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   a. Efectuar a operação de comutação com o `-simulate` parâmetro:

      `metrocluster switchover -simulate`

   b. Voltar ao nível de privilégio de administrador:

      `set -privilege admin`

6. Para configurações IP do MetroCluster usando o serviço Mediador ONTAP, confirme se o serviço Mediador está funcionando.

   a. Verifique se os discos Mediator estão visíveis para o sistema:

      `storage failover mailbox-disk show`

      O exemplo a seguir mostra que os discos da caixa de correio foram reconhecidos.

```
node_A_1::*> storage failover mailbox-disk show
                 Mailbox
Node             Owner     Disk    Name        Disk UUID
-------------     ------   -----   -----        ---------------
sti113-vsim-ucs626g
.
.
     local     0m.i2.3L26
7BBA77C9:AD702D14:831B3E7E:0B0730EE:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i2.3L27
928F79AE:631EA9F9:4DCB5DE6:3402AC48:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i1.0L60
B7BCDB3C:297A4459:318C2748:181565A3:00000000:00000000:00000000:000000
00:00000000:00000000
.
.
.
     partner   0m.i1.0L14
EA71F260:D4DD5F22:E3422387:61D475B2:00000000:00000000:00000000:000000
00:00000000:00000000
     partner   0m.i2.3L64
4460F436:AAE5AB9E:D1ED414E:ABF811F7:00000000:00000000:00000000:000000
00:00000000:00000000
28 entries were displayed.
```

b. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

c. Verifique se os LUNs da caixa de correio estão visíveis para o sistema:

   ```
   storage iscsi-initiator show
   ```

   A saída mostrará a presença dos LUNs da caixa de correio:

```
Node    Type       Label      Target Portal     Target Name
Admin/Op
----    ----       --------   ---------    ---------
--------------------------------       --------
.
.
.
.node_A_1
               mailbox
                     mediator 172.16.254.1    iqn.2012-
05.local:mailbox.target.db5f02d6-e3d3    up/up
.
.
.
17 entries were displayed.
```

a. Voltar ao nível de privilégio administrativo:

```
set -privilege admin
```

Recuperando-se de uma falha não controladora

Depois que o equipamento no local de desastre tiver sido submetido a qualquer manutenção ou substituição necessária, mas nenhum controlador tiver sido substituído, você poderá iniciar o processo de devolução da configuração do MetroCluster para um estado totalmente redundante. Isso inclui a recuperação da configuração (primeiro os agregados de dados e depois os agregados raiz) e a execução da operação de switchback.

Antes de começar

- Todo o hardware do MetroCluster no cluster de desastre deve estar funcional.
- A configuração geral do MetroCluster deve estar em switchover.
- Em uma configuração de MetroCluster conetada à malha, o ISL deve estar ativo e operar entre os locais do MetroCluster.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao executar este procedimento:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione uma mensagem de manutenção do AutoSupport antes e depois da manutenção para desativar a criação de casos durante a atividade de manutenção.

  Consulte o artigo da base de dados de Conhecimento "Como suprimir a criação automática de casos durante as janelas de manutenção programada".

- Ative o registo de sessão para qualquer sessão CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" no artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP".

Recuperação da configuração em uma configuração do MetroCluster

Nas configurações do MetroCluster FC, você realiza as operações de recuperação em uma ordem específica para restaurar o recurso MetroCluster após um switchover.

Nas configurações do MetroCluster IP, as operações de recuperação devem começar automaticamente após um switchover. Se eles não fizerem isso, você pode executar as operações de cura manualmente.

Antes de começar

- O switchover deve ter sido realizado e o local sobrevivente deve estar fornecendo dados.
- Os nós no local de desastre devem ser interrompidos ou permanecer desligados.

  Eles não devem ser totalmente inicializados durante o processo de cura.

- O storage no local de desastre deve estar acessível (as prateleiras são ativadas, funcionais e acessíveis).
- Nas configurações MetroCluster conetadas à malha, os links entre switches (ISLs) devem estar ativos e operacionais.
- Em configurações de MetroCluster de quatro nós, os nós do local que sobrevive não devem estar no estado de failover de HA (todos os nós precisam estar ativos e em execução para cada par de HA).

Sobre esta tarefa

A operação de recuperação deve primeiro ser realizada nos agregados de dados e, em seguida, nos agregados de raiz.

Recuperação dos agregados de dados

Você deve curar os agregados de dados após reparar e substituir qualquer hardware no local de desastre. Esse processo ressincroniza os agregados de dados e prepara o local de desastre (agora reparado) para operação normal. Você precisa curar os agregados de dados antes de curar os agregados de raiz.

Sobre esta tarefa

O exemplo a seguir mostra um switchover forçado, onde você coloca o agregado comutado on-line. Todas as atualizações de configuração no cluster remoto replicam com sucesso para o cluster local. Você liga o storage no local de desastre como parte deste procedimento, mas não deve nem ligar os módulos do controlador no local de desastre.

Passos

1. Verifique se o switchover foi concluído:

   ```
   metrocluster operation show
   ```

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. Ressincronize os agregados de dados executando o seguinte comando do cluster sobrevivente:

   `metrocluster heal -phase aggregates`

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

   Se a cura for vetada, você tem a opção de reemitir o `metrocluster heal` comando com o `--override-vetoes` parâmetro. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

3. Verifique se a operação foi concluída:

   `metrocluster operation show`

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Verifique o estado dos agregados:

   `storage aggregate show` comando.

```
controller_A_1::> storage aggregate show
Aggregate Size     Available Used% State   #Vols  Nodes        RAID
Status
--------- -------- --------- ----- ------- ------ ------------
------------
...
aggr_b2   227.1GB  227.1GB   0%    online  0      mcc1-a2      raid_dp,
mirrored, normal...
```

5. Se o storage tiver sido substituído no local de desastre, talvez seja necessário espelhar novamente os agregados.

Cura dos agregados de raiz após um desastre

Depois que os agregados de dados tiverem sido curados, você deve curar os agregados de raiz em preparação para a operação de switchback.

Antes de começar

A fase de agregados de dados do processo de recuperação do MetroCluster deve ter sido concluída com sucesso.

Passos

1. Volte a alternar os agregados espelhados:

   `metrocluster heal -phase root-aggregates`

   ```
   mcc1A::> metrocluster heal -phase root-aggregates
   [Job 137] Job succeeded: Heal Root Aggregates is successful
   ```

   Se a cura for vetada, você tem a opção de reemitir o `metrocluster heal` comando com o `--override-vetoes` parâmetro. Se você usar esse parâmetro opcional, o sistema substituirá quaisquer vetos de software que impeçam a operação de recuperação.

2. Certifique-se de que a operação de cura está concluída executando o seguinte comando no cluster de destino:

   `metrocluster operation show`

   ```
   mcc1A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

Verificando se o sistema está pronto para um switchback

Se o seu sistema já estiver no estado de comutação, você pode usar a `-simulate` opção para visualizar os resultados de uma operação de switchback.

Passos

1. Ligue cada módulo do controlador no local de desastre.

   Se os nós estiverem desligados:

   Ligue os nós.

   Se os nós estiverem no prompt Loader:

   Execute o comando: `boot_ontap`

2. Após a conclusão da inicialização do nó, verifique se os agregados raiz estão espelhados.

   Se ambos os plexos estiverem presentes, qualquer ressincronização será iniciada automaticamente. Se um Plex falhar, destrua-o e restabeleça a relação do espelho utilizando o seguinte comando para recriar o espelho:

   ```
   storage aggregate mirror -aggregate <aggregate-name>
   ```

3. Simule a operação de switchback:

   a. A partir do prompt de qualquer nó sobrevivente, altere para o nível de privilégio avançado:

      ```
      set -privilege advanced
      ```

   Você precisa responder com `y` quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   a. Execute a operação de switchback com o `-simulate` parâmetro:

      ```
      metrocluster switchback -simulate
      ```

   b. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

4. Revise a saída que é retornada.

   A saída mostra se a operação de switchback seria executada em erros.

Exemplo de resultados de verificação

O exemplo a seguir mostra a verificação bem-sucedida de uma operação de switchback:

```
cluster4::*> metrocluster switchback -simulate
  (metrocluster switchback)
[Job 130] Setting up the nodes and cluster components for the switchback
operation...DBG:backup_api.c:327:backup_nso_sb_vetocheck : MetroCluster
Switch Back
[Job 130] Job succeeded: Switchback simulation is successful.

cluster4::*> metrocluster op show
  (metrocluster operation show)
  Operation: switchback-simulate
      State: successful
 Start Time: 5/15/2014 16:14:34
   End Time: 5/15/2014 16:15:04
     Errors: -

cluster4::*> job show -name Me*
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
130    MetroCluster Switchback
                            cluster4
                                       cluster4-01
                                                      Success
       Description: MetroCluster Switchback Job - Simulation
```

Executando um switchback

Depois de curar a configuração do MetroCluster, você pode executar a operação MetroCluster switchback. A operação de switchback do MetroCluster retorna a configuração ao seu estado operacional normal, com as máquinas virtuais de armazenamento de origem sincronizada (SVMs) no local de desastre ativas e fornecendo dados dos pools de discos locais.

Antes de começar

- O cluster de desastres deve ter mudado com sucesso para o cluster sobrevivente.
- A recuperação deve ter sido realizada nos agregados de dados e raiz.
- Os nós de cluster sobreviventes não devem estar no estado de failover de HA (todos os nós precisam estar ativos e em execução para cada par de HA).
- Os módulos do controlador do local de desastre devem ser completamente inicializados e não no modo de aquisição de HA.
- O agregado raiz deve ser espelhado.
- Os links interswitches (ISLs) devem estar online.
- Todas as licenças necessárias devem ser instaladas no sistema.

Passos

1. Confirme se todos os nós estão no estado ativado:

```
metrocluster node show
```

O exemplo a seguir exibe os nós que estão no estado "habilitado":

```
cluster_B::>  metrocluster node show

DR                        Configuration  DR
Group Cluster Node        State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Confirme se a ressincronização está concluída em todos os SVMs:

   ```
   metrocluster vserver show
   ```

3. Verifique se todas as migrações automáticas de LIF que estão sendo executadas pelas operações de recuperação foram concluídas com sucesso:

   ```
   metrocluster check lif show
   ```

4. Execute o switchback executando o seguinte comando a partir de qualquer nó no cluster sobrevivente.

   ```
   metrocluster switchback
   ```

5. Verifique o progresso do funcionamento do interrutor de comutação:

   ```
   metrocluster show
   ```

   A operação de switchback ainda está em andamento quando a saída exibe "Waiting-for-switchback":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

A operação de comutação está concluída quando a saída exibe "normal":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se um switchback levar muito tempo para terminar, você pode verificar o status das linhas de base em andamento usando o seguinte comando no nível avançado de privilégio.

```
metrocluster config-replication resync-status show
```

6. Restabelecer qualquer configuração SnapMirror ou SnapVault.

   No ONTAP 8,3, você precisa restabelecer manualmente uma configuração de SnapMirror perdida após uma operação de switchback MetroCluster. No ONTAP 9.0 e mais tarde, o relacionamento é restabelecido automaticamente.

Verificando um switchback bem-sucedido

Depois de executar o switchback, você deseja confirmar que todos os agregados e máquinas virtuais de storage (SVMs) são trocados de volta e on-line.

Passos

1. Verifique se os agregados de dados comutados estão invertidos:

   ```
   storage aggregate show
   ```

   No exemplo a seguir, aggr_B2 no nó B2 mudou de volta:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Se o local de desastre incluiu agregados sem espelhamento e os agregados sem espelhamento não estiverem mais presentes, o agregado pode aparecer com um estado de "desconhecido" na saída `storage aggregate show` do comando. Contacte o suporte técnico para remover as entradas desatualizadas para os agregados sem espelhamento e consulte o artigo da base de dados de Conhecimento "Como remover entradas agregadas sem espelhamento obsoletas em um MetroCluster após desastre em que o armazenamento foi perdido."

2. Verifique se todos os SVMs de destino de sincronização no cluster sobrevivente estão inativos (mostrando um estado de administrador de "parado") e os SVMs de origem de sincronização no cluster de desastres estão ativos e em execução:

   `vserver show -subtype sync-source`

```
node_B_1::> vserver show -subtype sync-source
                                Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                                running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                                Admin      Root
Name    Name
Vserver             Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------         ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                       stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Os agregados de destino de sincronização na configuração do MetroCluster têm o sufixo "-mc" automaticamente anexado ao seu nome para ajudar a identificá-los.

3. Confirme se as operações de switchback foram bem-sucedidas:

   `metrocluster operation show`

Se o comando output mostrar…	Então…
Que o estado de operação de comutação é bem-sucedido.	O processo de switchback está concluído e você pode prosseguir com a operação do sistema.
Que a operação ou operação de comutação `switchback-continuation-agent` é parcialmente bem-sucedida.	Execute a correção sugerida fornecida na saída do `metrocluster operation show` comando.

Depois de terminar

Você deve repetir as seções anteriores para executar o switchback na direção oposta. Se o site_A fez um

switchover do site_B, faça um switchover do site_A.

Excluindo listagens agregadas obsoletas após o switchback

Em algumas circunstâncias após o switchback, você pode notar a presença de agregados *stale*. Agregados obsoletos são agregados que foram removidos do ONTAP, mas cujas informações permanecem registradas no disco. Agregados obsoletos são exibidos com o `nodeshell aggr status -r` comando, mas não com o `storage aggregate show` comando. Você pode excluir esses Registros para que eles não apareçam mais.

Sobre esta tarefa

Agregados obsoletos podem ocorrer se você relocou agregados enquanto a configuração do MetroCluster estava em switchover. Por exemplo:

1. Local A muda para local B..
2. Você exclui o espelhamento de um agregado e reposiciona o agregado de node_B_1 para node_B_2 para balanceamento de carga.
3. Você executa a recuperação agregada.

Neste ponto, um agregado obsoleto aparece em node_B_1, mesmo que o agregado real tenha sido excluído desse nó. Esse agregado aparece na saída do `nodeshell aggr status -r` comando. Ele não aparece na saída `storage aggregate show` do comando.

1. Compare a saída dos seguintes comandos:

   `storage aggregate show`

   `run local aggr status -r`

   Agregados obsoletos aparecem na `run local aggr status -r` saída, mas não na `storage aggregate show` saída. Por exemplo, o seguinte agregado pode aparecer na `run local aggr status -r` saída:

```
Aggregate aggr05 (failed, raid_dp, partial) (block checksums)
Plex /aggr05/plex0 (offline, failed, inactive)
  RAID group /myaggr/plex0/rg0 (partial, block checksums)

 RAID Disk Device  HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)
Phys (MB/blks)
 --------- ------  ------------- ---- ---- ----  ----- --------------
--------------
 dparity   FAILED          N/A                        82/ -
 parity    0b.5    0b    -   -   SA:A   0 VMDISK  N/A 82/169472
88/182040
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 Raid group is missing 7 disks.
```

2. Remova o agregado obsoleto:

   a. No prompt de qualquer nó, altere para o nível de privilégio avançado:

      ```
      set -privilege advanced
      ```

   Você precisa responder com `y` quando solicitado para continuar no modo avançado e ver o prompt do modo avançado (*>).

   a. Remova o agregado obsoleto:

      ```
      aggregate remove-stale-record -aggregate aggregate_name
      ```

   b. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

3. Confirme que o registo agregado obsoleto foi removido:

   ```
   run local aggr status -r
   ```

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/"

Informações de segurança e avisos regulamentares

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Informações sobre direitos autorais

Informações sobre marcas comerciais