



Instale um MetroCluster conectado à malha

ONTAP MetroCluster

NetApp
January 10, 2025

Índice

Instale um MetroCluster conectado à malha	1
Visão geral	1
Prepare-se para a instalação do MetroCluster	1
Escolhendo o procedimento de instalação correto para sua configuração	11
Cable uma configuração de MetroCluster conectada à malha	13
Configurar o hardware para compartilhar uma malha Brocade 6510 FC durante a transição	199
Configurando o software MetroCluster no ONTAP	208
Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster	268
Testando a configuração do MetroCluster	271
Considerações ao remover configurações do MetroCluster	290
Planejar e instalar uma configuração MetroCluster com LUNs de array	291
Como usar o Active IQ Unified Manager e o Gerenciador de sistemas ONTAP para configuração e monitoramento adicionais	346
Considerações ao usar o ONTAP em uma configuração do MetroCluster	347
Onde encontrar informações adicionais	359

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 conectividade entre os requisitos de porta, endereço IP, sub-rede, firewall e nomenclatura de cluster é atendida.

Requisitos de conectividade

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 conectividade 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 aspectos 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 aspectos da sua rede para determinar se o compartilhamento de portas de dados é a melhor solução de conectividade 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 conectados aos switches compartilhados.

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

- Dispositivos que não sejam MetroCluster não devem ser conectados 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	<ul style="list-style-type: none"> • AptPolicy deve ser definido como 1 • O DLS tem de estar definido como Off (Desligado) • IOD deve ser definido como On (ligado) 	<ul style="list-style-type: none"> • AptPolicy deve ser definido como 3 • O DLS tem de estar definido para ON (ligado) • IOD deve ser definido como Off (Desligado)
Cisco	<p>Políticas para o VSAN designado pela FCVI:</p> <ul style="list-style-type: none"> • Política de balanceamento de carga: Srcid e dstid • IOD deve ser definido como On (ligado) <p>Políticas para o VSAN designado para armazenamento:</p> <ul style="list-style-type: none"> • 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 conectividade MetroCluster de back-end não deve ser usado para qualquer outra conectividade.

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

- Uma placa de linha pode ser conectada 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

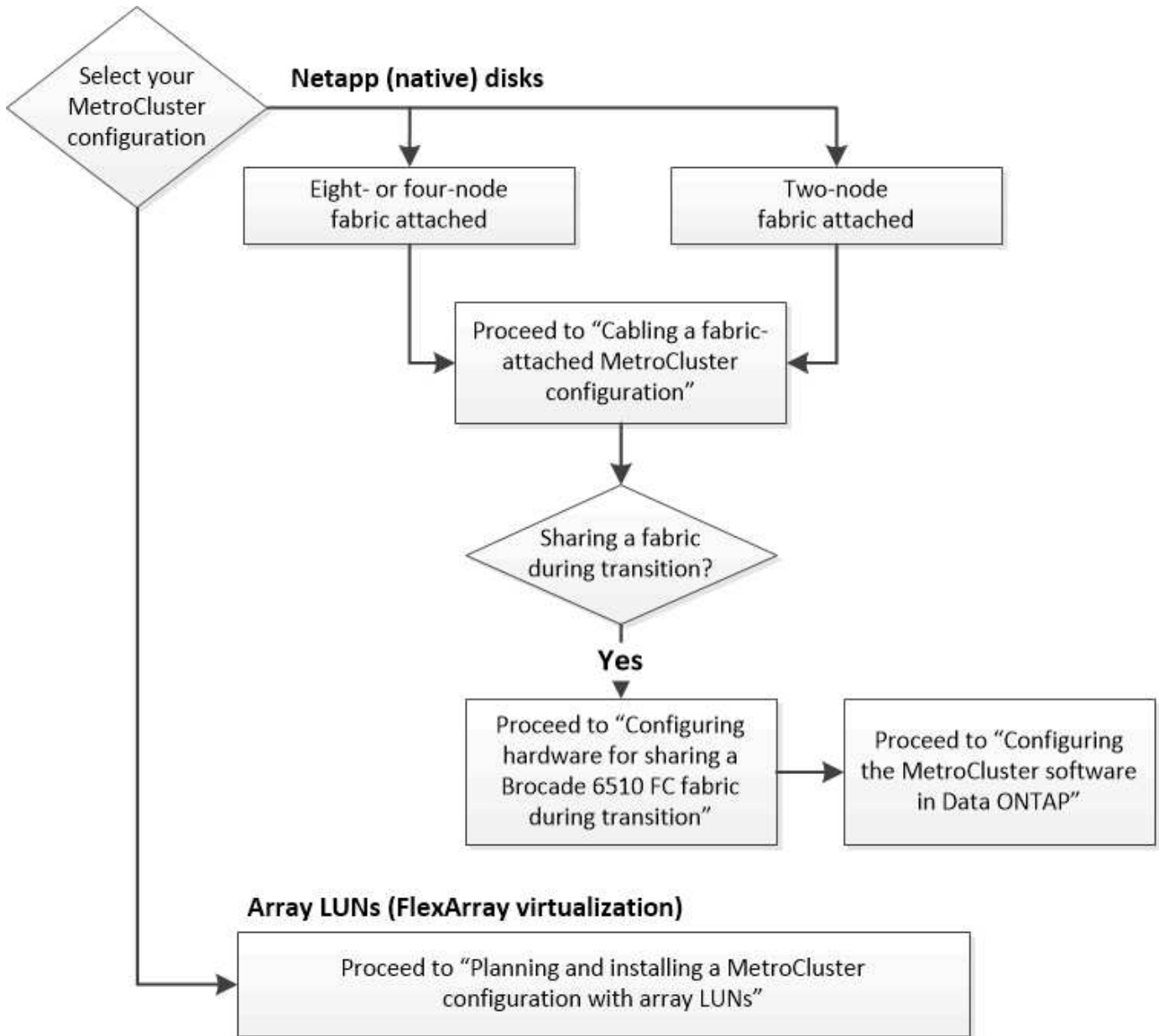
Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o acesso às portas necessárias.

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)	<ol style="list-style-type: none"> 1. "Fazer o cabeamento de uma configuração MetroCluster conectada à malha" 2. "Configurando o software MetroCluster no ONTAP"
<p>Configuração conectada à malha ao compartilhar com uma malha de switch FC existente</p> <p>Isso é suportado apenas como uma configuração temporária com uma configuração de MetroCluster de malha de 7 modos usando os switches Brocade 6510.</p>	<ol style="list-style-type: none"> 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

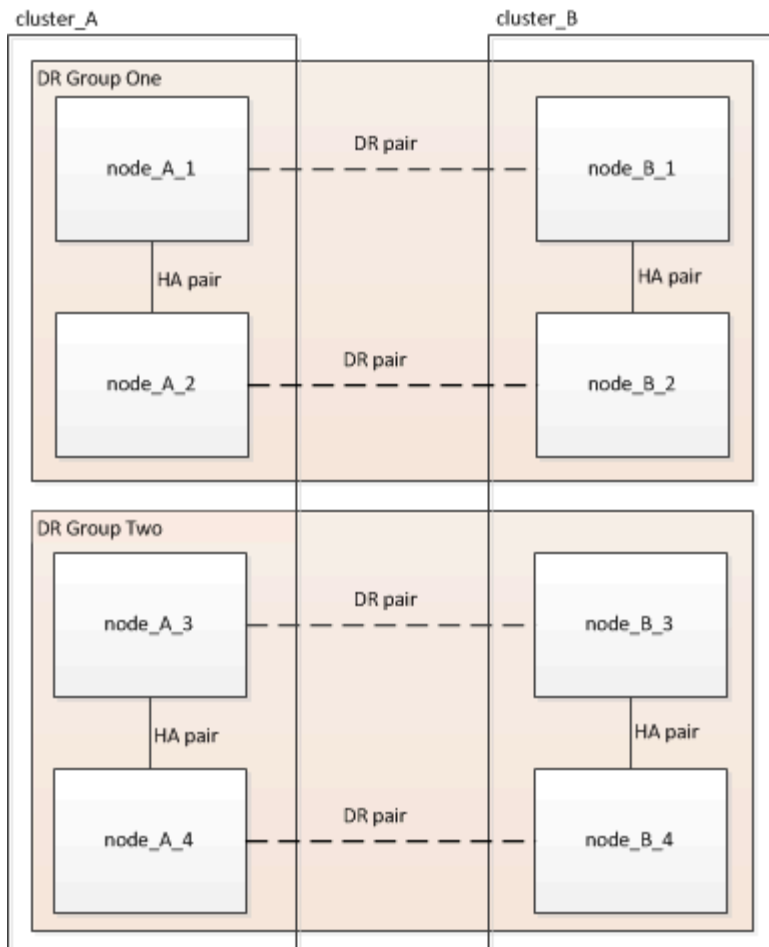
Ao Planejar sua configuração do MetroCluster, você deve entender os componentes de hardware e como eles se interconectam.

Grupos de recuperação de desastres (DR)

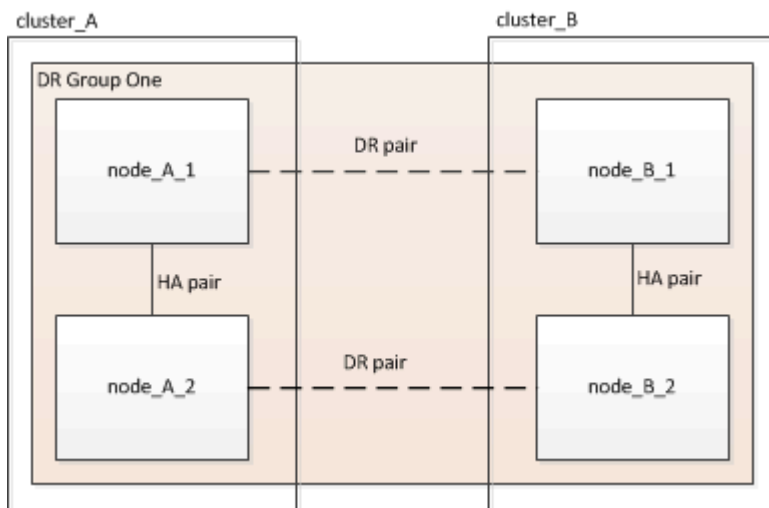
Uma configuração do Fabric MetroCluster consiste em um ou dois grupos de DR, dependendo do número de nós na configuração do MetroCluster. Cada grupo de DR consiste em quatro nós.

- 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 conectividade 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.

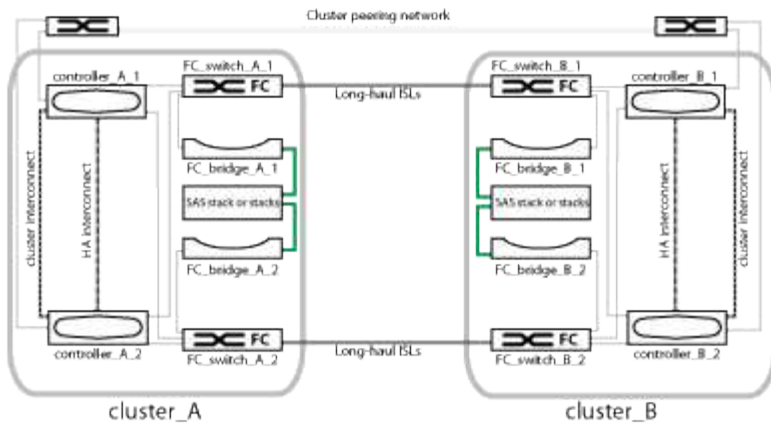
- Conexões Ethernet dos controladores para a rede fornecida pelo cliente que é usada para peering de cluster

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

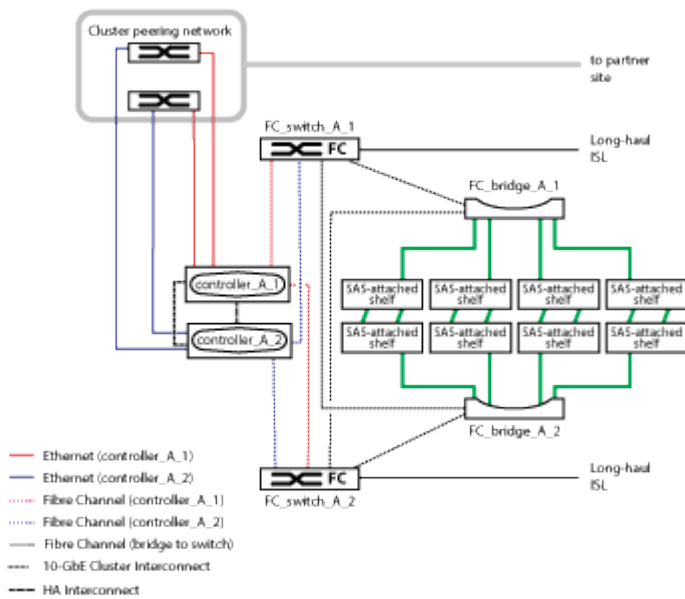
- Uma interconexão de cluster entre cada controlador no cluster local

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.

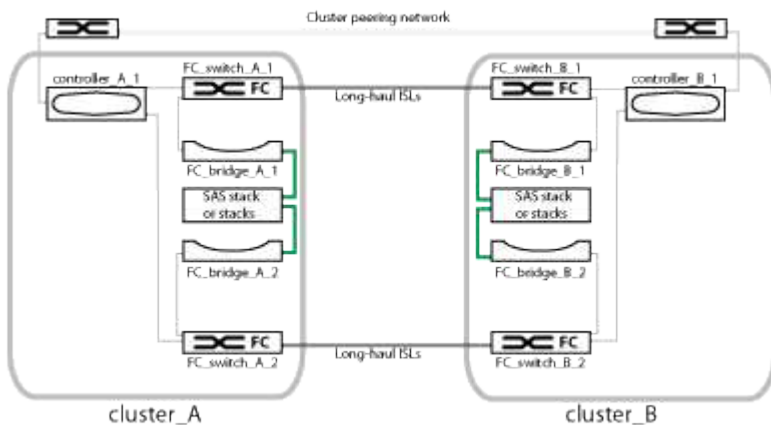


A ilustração a seguir mostra uma visão mais detalhada da conectividade em um único cluster MetroCluster (ambos os clusters têm a mesma configuração):



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.

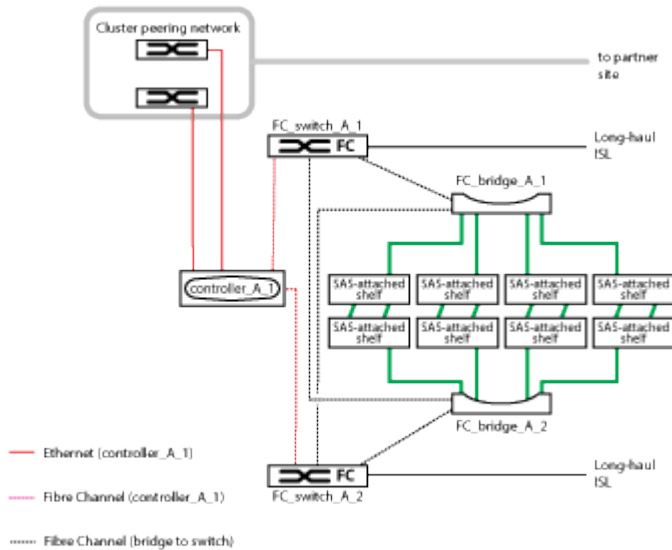


Uma configuração de dois nós consiste em dois clusters, um em cada local geograficamente separado. O cluster_A está localizado no primeiro site do MetroCluster. O cluster_B está localizado no segundo site do MetroCluster. Cada local tem uma pilha de storage SAS. São suportadas stacks de armazenamento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

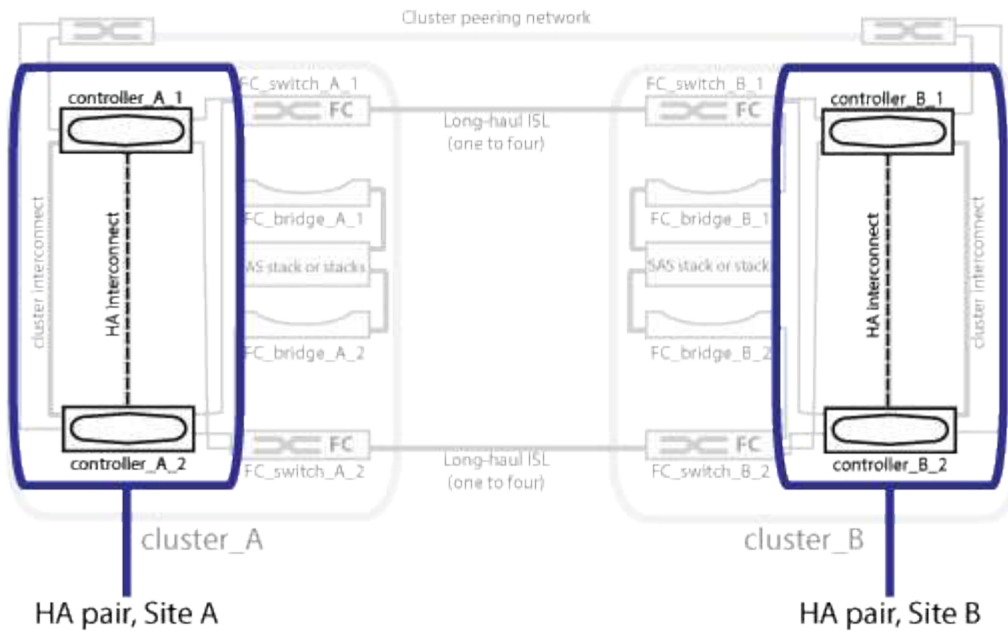
- Conexões FC entre o adaptador FC-VI em cada módulo de controladora
- Conexões FC de HBAs de cada módulo de controladora à ponte FC-para-SAS para cada stack de gaveta SAS
- Conexões SAS entre cada compartimento SAS e da parte superior e inferior de cada stack até uma ponte FC para SAS
- Conexões Ethernet 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"

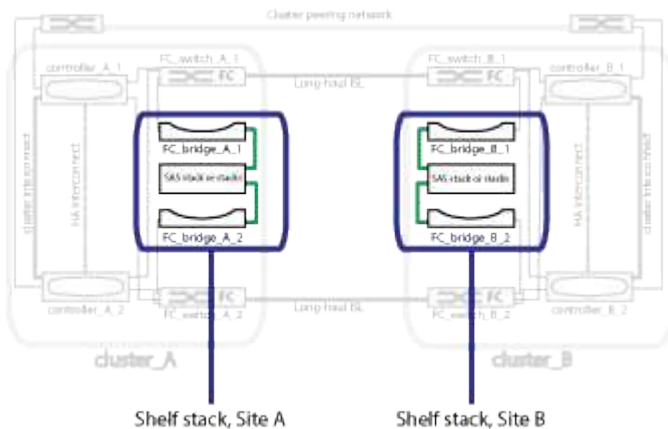
"Malhas de switches FC redundantes"

"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

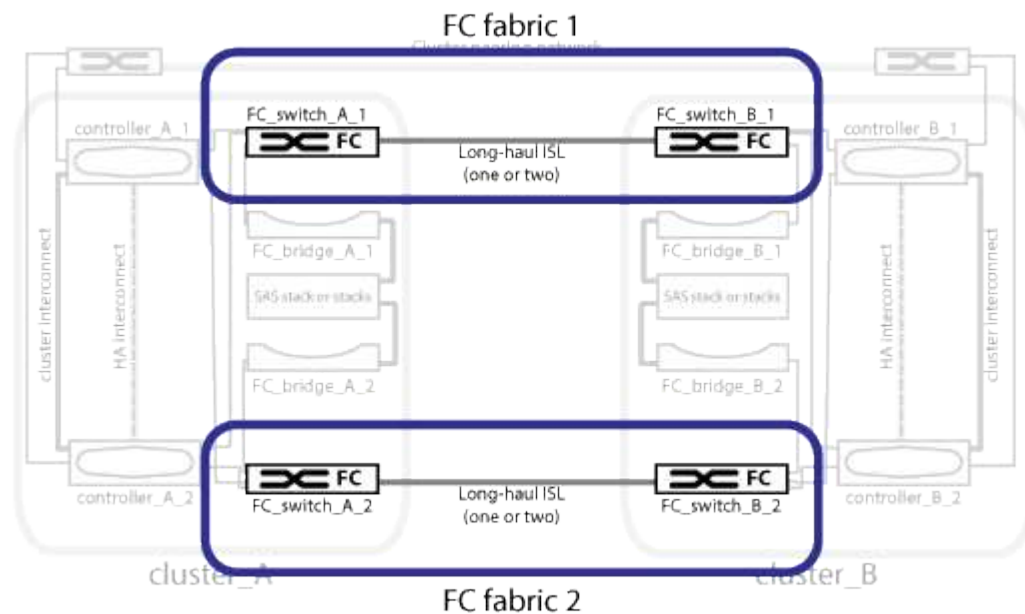
"Ilustração dos pares de HA locais em uma configuração do MetroCluster"

"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"](#)

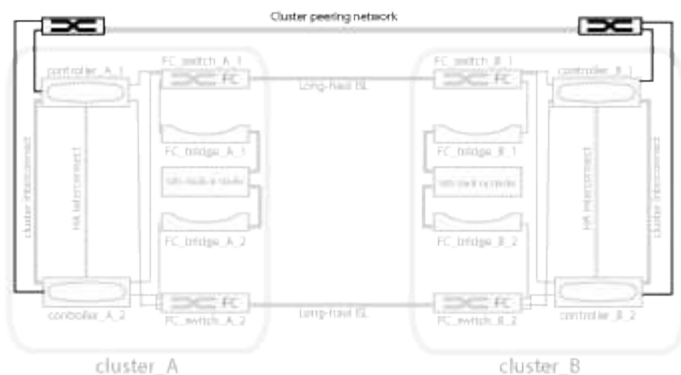
["Ilustração de pontes FC para SAS redundantes"](#)

["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 conectadas 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 SFPs 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 conecta, 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 conecta. 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 conecta 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. Conecte 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 conectar os switches FC em cada local por meio dos links interswitches (ISLs) de fibra ótica para formar as malhas de switch que conectam os componentes do MetroCluster.

Sobre esta tarefa

Isso deve ser feito para ambos os tecidos de troca.

Passos

1. Conecte 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, conecte apenas dois iniciadores e deixe os outros dois conectados 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 conectar 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 seção 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 interruptor 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		
		Liga ao interruptor 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

Componente	Porta	Liga ao FC_switch ...	Modelo de interruptor Brocade				
			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_54 b	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 interruptor 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 interruptor	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 posterior](#) consulte .

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 conectadas 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 conectadas 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 conectadas 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 posterior](#) consulte .

Modelo do interruptor	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_3a	FC1
1	LEM2-11	FC2	2
LEM2-11	ponte_x_3b	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 conectar 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 seção 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 interruptor 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 interruptor 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_5 1a	FC1	1	32	-	26	26	32
		FC2	2	32	-	26	26	32
	bridge_x_5 1b	FC1	1	33	-	27	27	33
		FC2	2	33	-	27	27	33
Pilha 2	bridge_x_5 2a	FC1	1	34	-	30	30	34
		FC2	2	34	-	30	30	34
	bridge_x_5 2b	FC1	1	35	-	31	31	35
		FC2	2	35	-	31	31	35
Pilha 3	bridge_x_5 3a	FC1	1	-	-	32	32	36
		FC2	2	-	-	32	32	36
	bridge_x_5 3b	FC1	1	-	-	33	33	37
		FC2	2	-	-	33	33	37

Empilha y	bridge_x_5 ya	FC1	1	-	-	34	34	38
		FC2	2	-	-	34	34	38
	bridge_x_5 yb	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 interruptor 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 interruptor 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 interruptor	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 interruptor 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 interruptor	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 conectividade 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 conectividade de rede é de 1 GbE.

Passo

1. Identifique e faça o cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conectividade 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 conectar 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	<ul style="list-style-type: none">• "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	<ul style="list-style-type: none">• "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 interruptor.
4. Desativar o interruptor:

```
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 interruptores 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 interruptor:

```
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 interruptores 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 interruptor:

- 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 interruptor:

- 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 computador.

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.

Transferir e instalar o software Cisco FC switch NX-os

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 interruptor para o interruptor:

```
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 interruptor:

```
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 interruptor reinicia automaticamente após a instalação do software do interruptor.

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

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 interruptor:

```
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 conectar 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 interruptor 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 interruptor:

```
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 interruptor 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 interruptor

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 conectadas 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 interruptor.
- 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:

```
aptopolicy 3
```

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

```
dlsreset
```

- iv. Verifique as configurações do AID:

```
iodshow
```

```
aptopolicy
```

```
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 interruptor.



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 interruptor.

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

a. Altere a cadeia de caracteres 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 interruptor:

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 interruptor num interruptor 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 interruptor	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:

$$1,5 \times \text{real_distance}: \text{distância}$$

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	Port Type	Lx Mode	Max/Resv Buffers	Buffer Usage	Needed Buffers	Link Distance	Remaining 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 interruptor 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 interruptor 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 interruptores:

- 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:

```
portcfg 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 interruptor:

```
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 interruptor 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 interruptor 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 interruptores 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 conectam 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 caracteres 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 conectando 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 conecta. 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 conecta 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 conectando dois grupos de pilha em cada local. Como cada ponte usa uma porta FC, há um total de oito zonas de storage por malha (dezesesseis 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 conecta. 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 conecta 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 interruptor:

```
switchdisable
```

2. Configure e defina a carga útil:

```
configure
```

3. Defina os seguintes parâmetros do interruptor:

- 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 interruptor:

```
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 Port	Encryption 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 conectividade 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 conectar 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 conectada 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 interruptor 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 interruptor.

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 caracteres 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 caracteres da comunidade como "public" (todas minúsculas) para permitir o acesso a partir dos monitores de saúde do ONTAP.

Você pode definir a cadeia de caracteres da comunidade para um valor diferente de "público", mas você deve configurar os monitores de integridade do ONTAP usando a cadeia de caracteres 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. Adquirir 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. Adquirir 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 interruptor 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 conectadas 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 interruptor 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 interruptor.

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 interruptor.

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 interruptor.

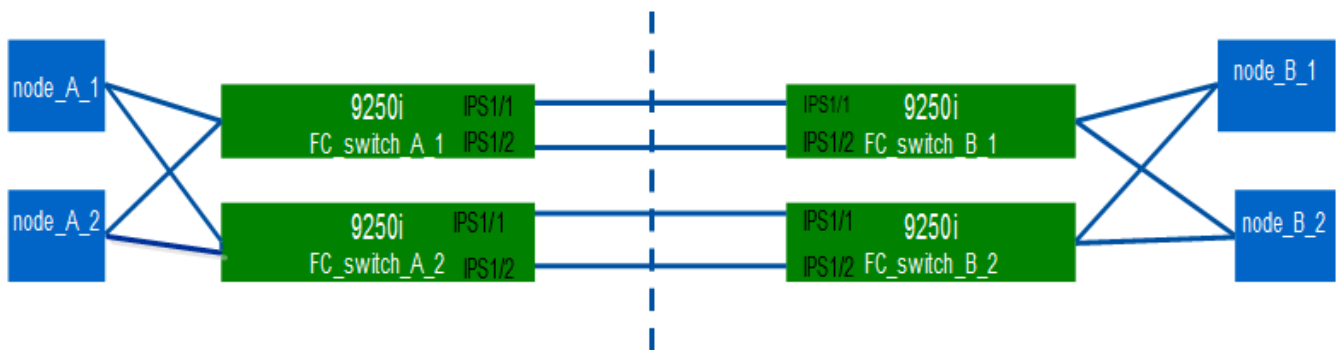
Configuração de portas FCIP para um ISL duplo em switches FC Cisco 9250i

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/3230	10
Armazena mento	fcip 2	20	3221	c.c.c.c/3231	20	IPStorage 1/2	b.b.b.b	FC-VI
fcip 3	25	3222	d.dd.d/3232	10	Armazena mento	fcip 4	30	3223

d.dd.d/3233	20	FC_switch_B_1	IPStorage 1/1	c.c.c.c	FC-VI	fcip 1	15	3230
a.a.a.a/3220	10	Armazenamento	fcip 2	20	3231	a.a.a.a/3221	20	IPStorage 1/2
d.d.d.d	FC-VI	fcip 3	25	3232	b.b.b.b/3222	10	Armazenamento	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/3230	10
Armazenamento	fcip 2	20	3221	1. g.g.g/3231	20	IPStorage 1/2	f.f.f.f	FC-VI
fcip 3	25	3222	h.h.h.h. h/3232	10	Armazenamento	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/3220	10	Armazenamento	fcip 2	20	3231	e.e.e.e/3221	20	IPStorage 1/2
h.h.h.h	FC-VI	fcip 3	25	3232	f.f. f/3222	10	Armazenamento	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 ativos 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

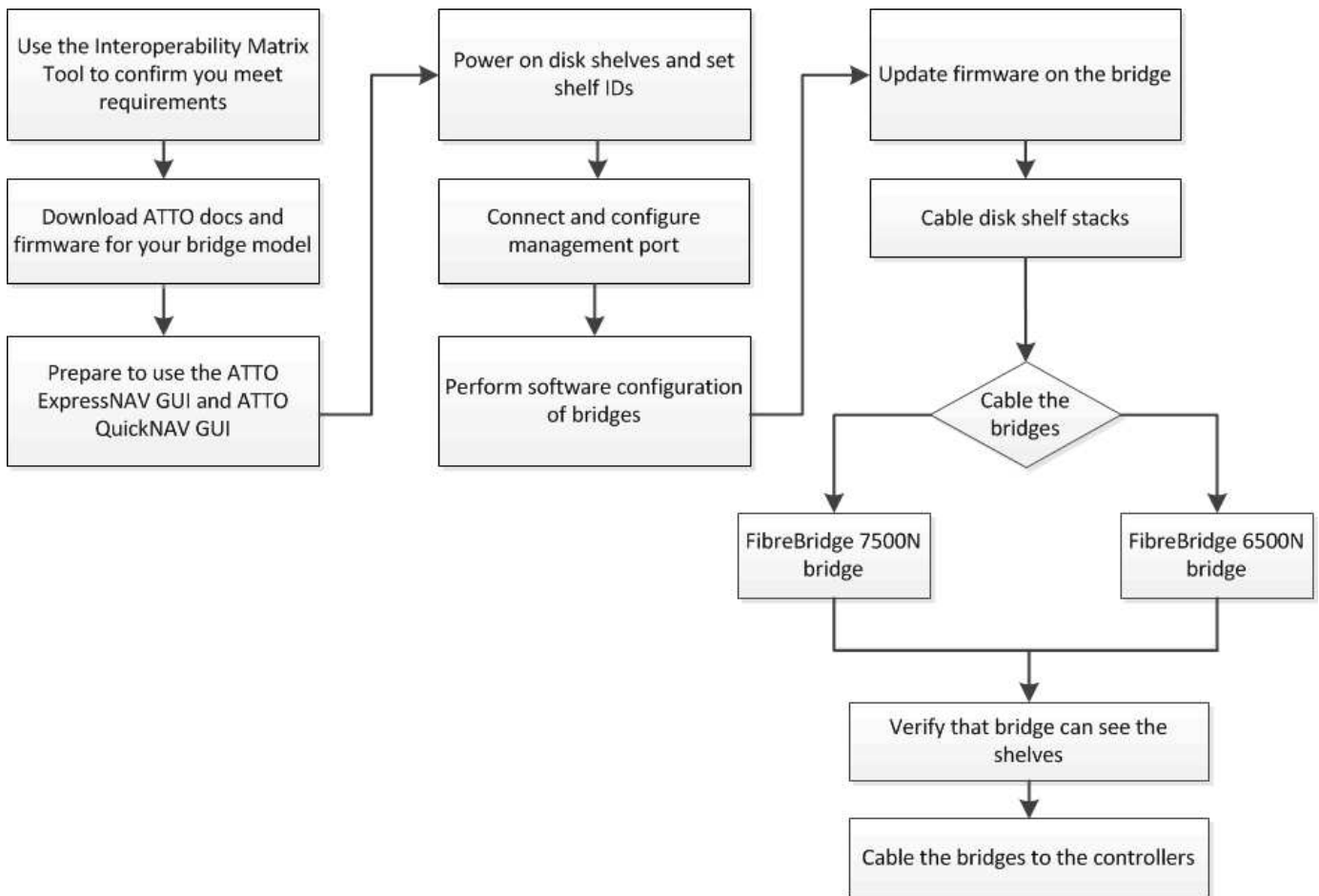
Para sistemas recebidos de fábrica, as pontes FC para SAS são pré-configuradas e não exigem configuração adicional.

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 conectividade 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 conectada 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 conecta 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 conectividade 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 micrones, 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 conectando 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 conecta. 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	<p>a. Veja o status das pontes:</p> <pre>storage bridge show</pre> <p>A saída mostra qual ponte não está protegida.</p> <p>b. Fixe a ponte:</p> <pre>securebridge</pre>
ONTAP 9 1.4 ou anterior	<p>a. Veja o status das pontes:</p> <pre>storage bridge show</pre> <p>A saída mostra qual ponte não está protegida.</p> <p>b. Verifique o estado das portas da ponte não protegida:</p> <pre>info</pre> <p>A saída mostra o status das portas Ethernet MP1 e MP2.</p> <p>c. Se a porta Ethernet MP1 estiver ativada, execute:</p> <pre>set EthernetPort mp1 disabled</pre> <p>Se a porta Ethernet MP2 também estiver ativada, repita a subetapa anterior para a porta MP2.</p> <p>d. Salve a configuração da ponte.</p> <p>Você deve executar os seguintes comandos:</p> <pre>SaveConfiguration</pre> <pre>FirmwareRestart</pre> <p>Você é solicitado a reiniciar a ponte.</p>

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 conector de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conector).

Passos

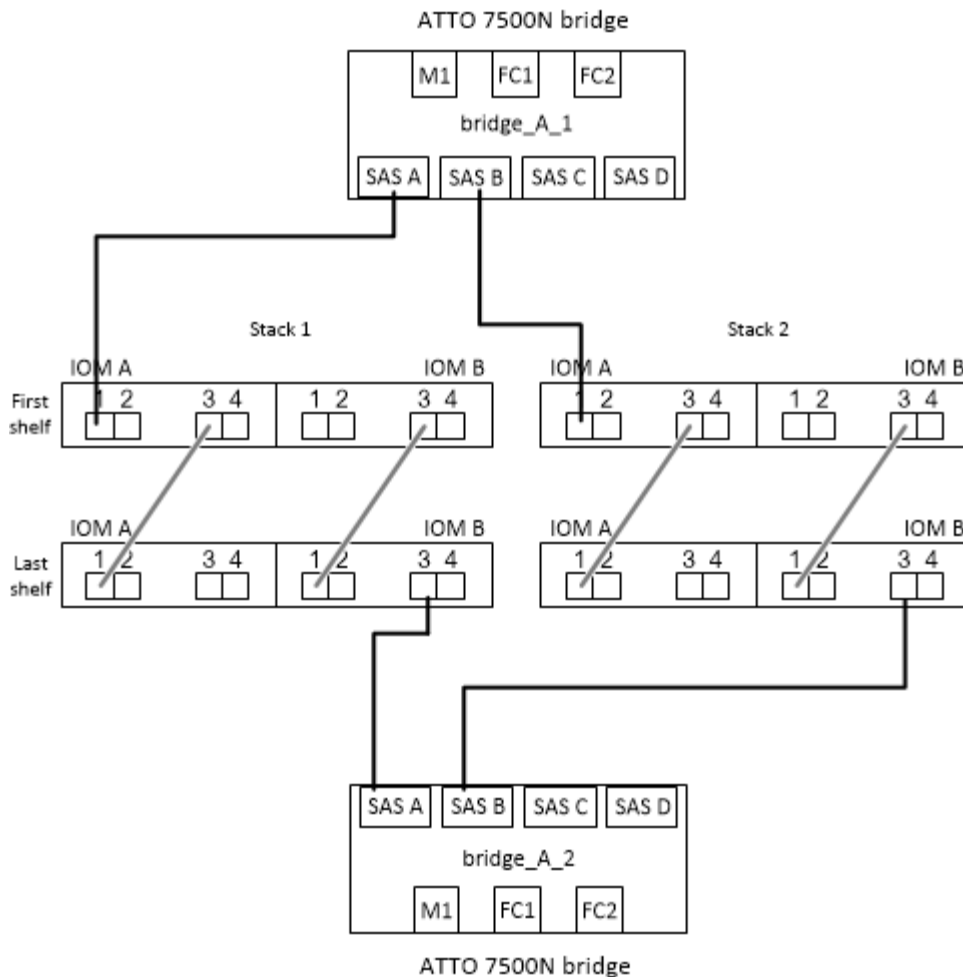
1. Encadeie em série as gavetas de disco em cada pilha:
 - a. Começando pela primeira gaveta lógica na stack, conecte IOM A porta 3 à IOM a porta 1 na próxima gaveta até que cada IOM A na stack seja conectada.
 - b. Repita o subpasso anterior para IOM B.
 - c. Repita as subetapas anteriores para cada 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, conecte as pilhas baseadas nos módulos IOM12 e IOM3/IOM6 à mesma ponte desde que estejam conectadas 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 conectadas 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 conectores 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 conector de cabo SAS com a aba de puxar orientada para baixo (na parte inferior do conector).

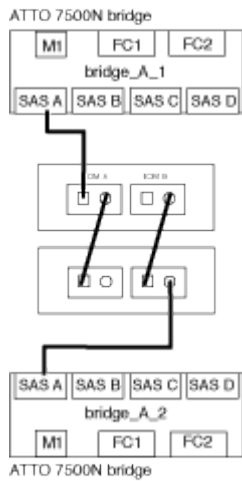
Passos

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.

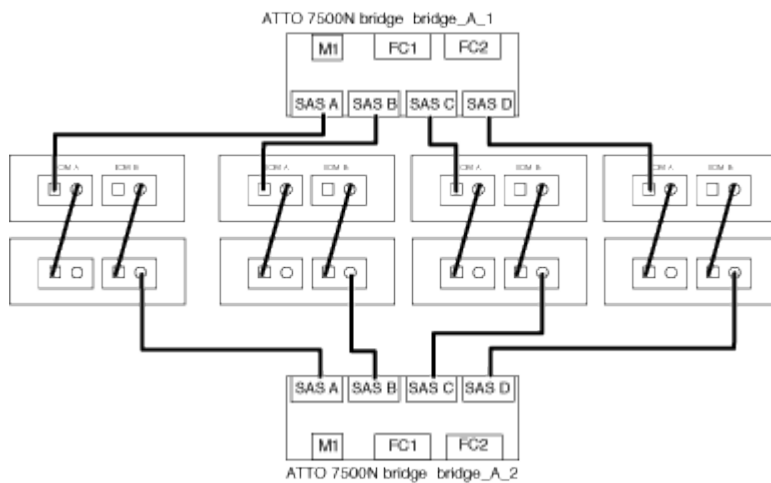
["Guia de instalação e serviço das gavetas de disco SAS para DS4243, DS2246, DS4486 e DS4246"](#)

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 detectar 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 detectar todas as unidades de disco e prateleiras de disco às quais está conetada:

Se você estiver usando O...	Então...
--------------------------------	----------

ATTO ExpressNAV GUI	<p>a. Em um navegador da Web compatível, insira o endereço IP de uma ponte na caixa do navegador.</p> <p>Você é levado para a página inicial DO ATTO FibreBridge da ponte para a qual você inseriu o endereço IP, que tem um link.</p> <p>b. Clique no link e insira seu nome de usuário e a senha que você designou quando configurou a ponte.</p> <p>A página de status ATTO FibreBridge da ponte é exibida com um menu à esquerda.</p> <p>c. Clique em Avançado.</p> <p>d. Visualize os dispositivos conectados usando o comando <code>sastargets</code> e clique em Submit.</p>
Conexão de porta serial	<p>Ver os dispositivos ligados:</p> <pre>sastargets</pre>

A saída mostra os dispositivos (discos e compartimentos de disco) aos quais a ponte está conectada. 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 conectados:

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	3QP1G7A900009939FNNT
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 conectar-se à ponte e digitar o mesmo comando para ver toda a saída.

- Verifique se a saída do comando mostra que a ponte está conectada a todos os discos e compartimentos de disco na pilha à qual deve ser conectada.

Se a saída for...	Então...
Correto	Repita Passo 1 para cada ponte restante.

Não está correto	<p>a. Verifique se há cabos SAS soltos ou corrija o cabeamento SAS repetindo o cabeamento.</p> <p>Cable disk shelves to the bridges</p> <p>b. Repita Passo 1.</p>
------------------	---

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 conectado 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 conectar 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 mirrored 64-bit	root, nosnap=on

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> cfsave
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 interruptores:

```
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 conectados 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
```

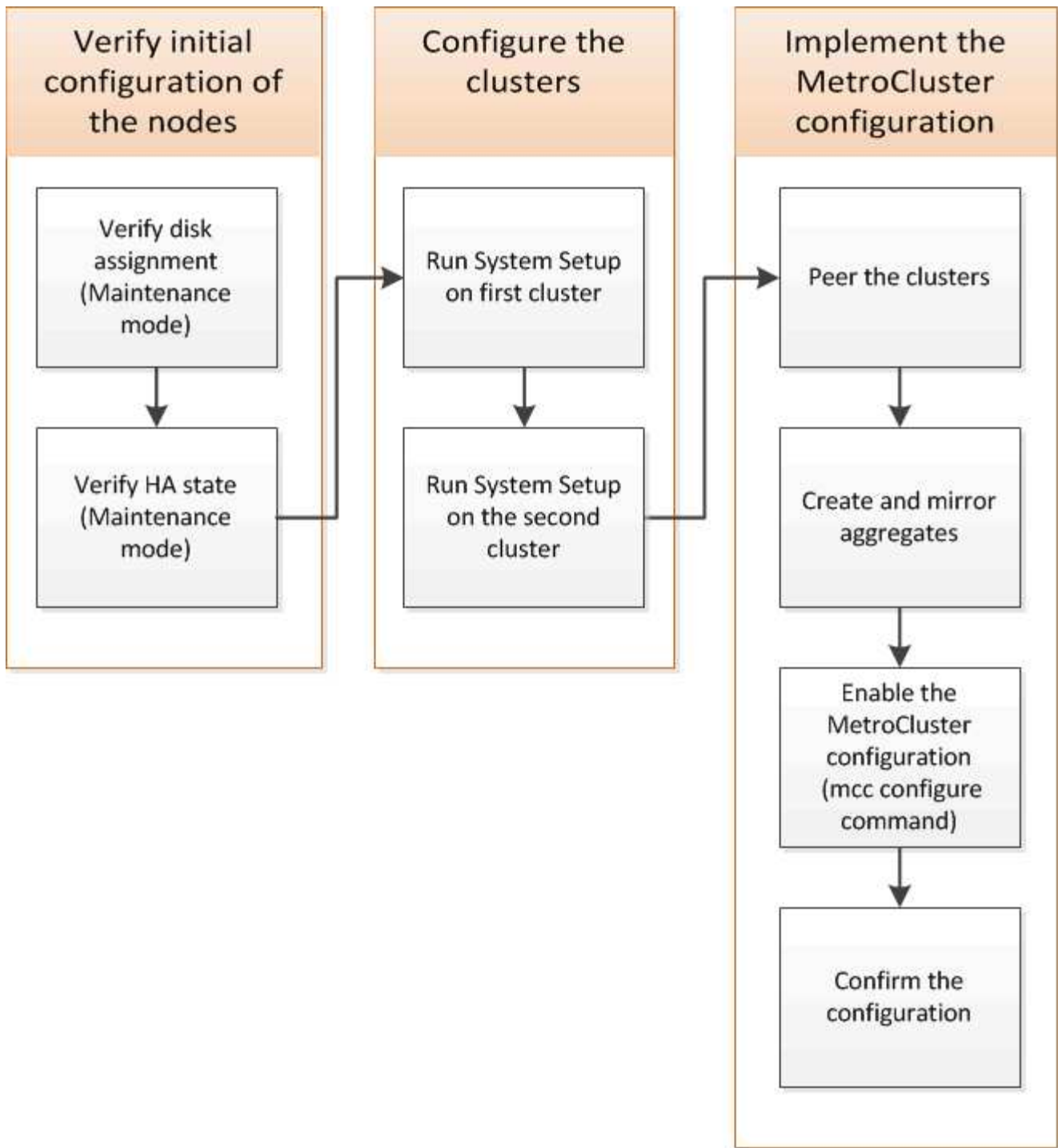
3. Execute o utilitário `fmc_dc` para garantir que o 7-Mode Fabric MetroCluster esteja funcionando corretamente.

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	<code>mcc</code>
Configuração de FC MetroCluster de dois nós	<code>mcc-2n</code>
Configuração IP MetroCluster de oito ou quatro nós	<code>mccip</code>

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	<code>ha-config modify controller mcc</code>

Configuração de FC MetroCluster de dois nós	<code>ha-config modify controller mcc-2n</code>
Configuração IP MetroCluster de oito ou quatro nós	<code>ha-config modify controller mccip</code>

- 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	<code>ha-config modify chassis mcc</code>
Configuração de FC MetroCluster de dois nós	<code>ha-config modify chassis mcc-2n</code>
Configuração IP MetroCluster de oito ou quatro nós	<code>ha-config modify chassis mccip</code>

- Inicialize o nó no ONTAP:

```
boot_ontap
```

- 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

- No prompt Loader, retorne as variáveis ambientais à configuração padrão:

```
set-defaults
```

- Inicialize o nó no modo Manutenção e, em seguida, configure as configurações para quaisquer HBAs no sistema:

- Arranque no modo de manutenção:

```
boot_ontap maint
```

- 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	<code>ucadmin modify -m fc -t initiator adapter_name</code>
CNA Ethernet	<code>ucadmin modify -mode cna adapter_name</code>
Destino de FC	<code>fcadmin config -t target adapter_name</code>
Iniciador FC	<code>fcadmin config -t initiator adapter_name</code>

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	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

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:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Verifique se as portas estão desativadas:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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 conectadas 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

```

(Mbps)		Speed				
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
```

Vserver	Group	Failover 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-addr peer_LIF_IPs -ipSPACE ipSPACE
```

Se você especificar ambos `-generate-passphrase` e `-peer-addr`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addr` 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-addr 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-addr  
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 conectividade 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-addr 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-addr 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-addr peer_LIF_IPs -ip-space ip-space
```

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-addr 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 conectividade 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 conectado 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 conectado 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	<p>A partir do prompt de qualquer nó, configure o MetroCluster:</p> <pre>metrocluster configure node-name</pre>
Um único agregado de dados espelhados	<p>a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado:</p> <pre>set -privilege advanced</pre> <p>Você precisa responder <code>y</code> quando for solicitado a continuar no modo avançado e você vir o prompt do modo avançado (<code>*></code>).</p> <p>b. Configure o MetroCluster com o <code>-allow-with-one-aggregate true</code> parâmetro:</p> <pre>metrocluster configure -allow-with-one-aggregate true node-name</pre> <p>c. Voltar ao nível de privilégio de administrador:</p> <pre>set -privilege admin</pre>



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
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) 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 ODE 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
```

Node	Adapter Name	Adapter Type	Link Status	Is OOD Enabled?	IP Address	Port Number
mcc4-b1 6a	fcvi_device_0	FC-VI	Up	false	17.0.1.2	
mcc4-b1 6b	fcvi_device_1	FC-VI	Up	false	18.0.0.2	
mcc4-b1 ib2a	mlx4_0	IB	Down	false	192.0.5.193	
mcc4-b1 ib2b	mlx4_0	IB	Up	false	192.0.5.194	
mcc4-b2 6a	fcvi_device_0	FC-VI	Up	false	17.0.2.2	
mcc4-b2 6b	fcvi_device_1	FC-VI	Up	false	18.0.1.2	
mcc4-b2 ib2a	mlx4_0	IB	Down	false	192.0.2.9	
mcc4-b2 ib2b	mlx4_0	IB	Up	false	192.0.2.10	

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

```

Node Port Number	Adapter Name	Adapter Type	Link Status	Is OOD Enabled?	IP Address
mcc4-b1 6a	fcvi_device_0	FC-VI	Up	false	17.0.1.2
mcc4-b1 6b	fcvi_device_1	FC-VI	Up	false	18.0.0.2
mcc4-b1 ib2a	mlx4_0	IB	Down	false	192.0.5.193
mcc4-b1 ib2b	mlx4_0	IB	Up	false	192.0.5.194
mcc4-b2 6a	fcvi_device_0	FC-VI	Up	false	17.0.2.2
mcc4-b2 6b	fcvi_device_1	FC-VI	Up	false	18.0.1.2
mcc4-b2 ib2a	mlx4_0	IB	Down	false	192.0.2.9
mcc4-b2 ib2b	mlx4_0	IB	Up	false	192.0.2.10

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

```

Node Number	Adapter Name	Adapter Type	Link Status	Is OOD Enabled?	IP Address	Port
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]
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 MetroCluster](#) consulte .



- 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_address> -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	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>

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 Model	Symbolic Name Bridge WWN	Is Monitored	Monitor Status	Vendor
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
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	

```

ok                                     mirroring-status
ok                                     disk-pool-allocation
ok                                     ownership-state

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:

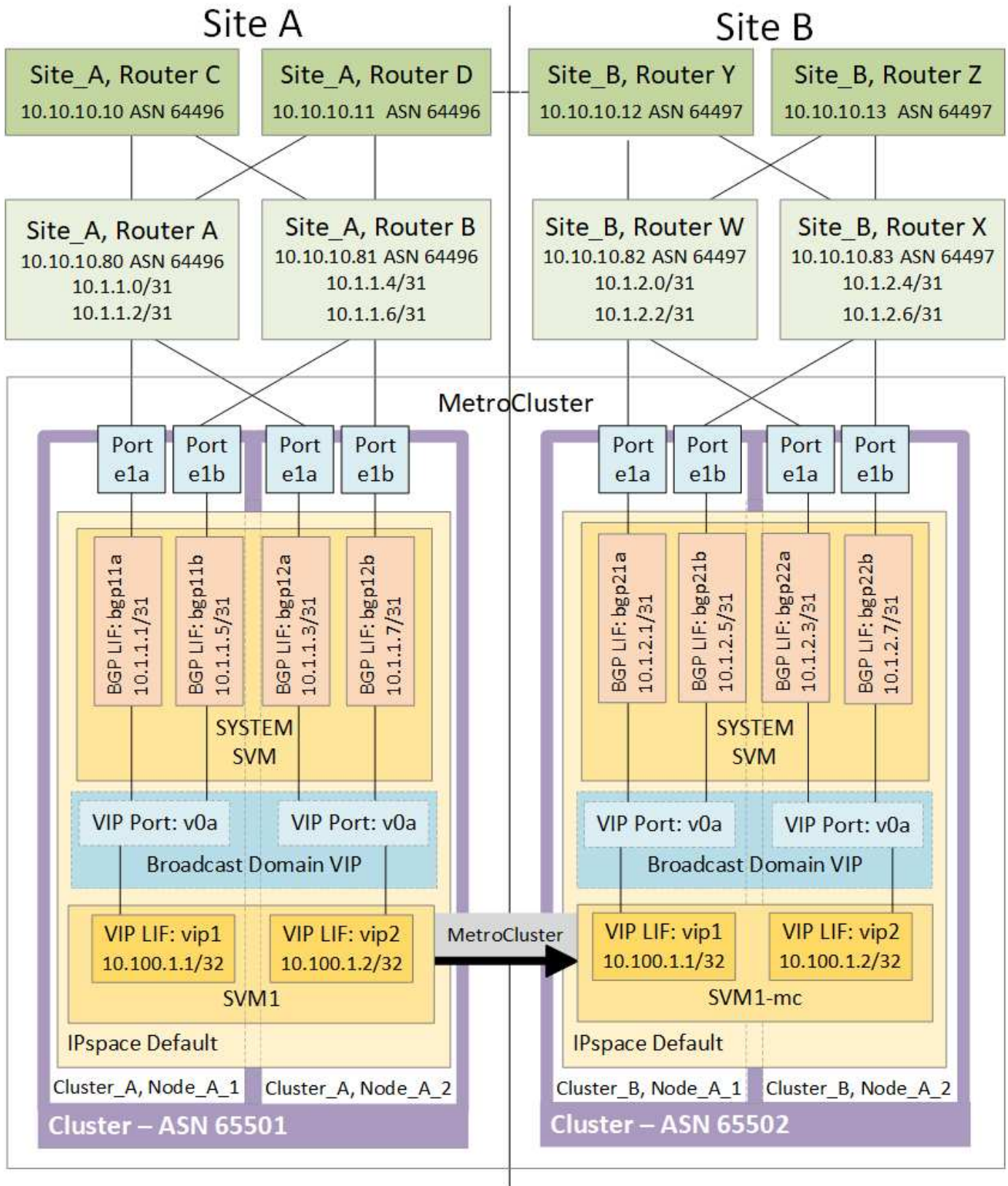
```
system configuration backup settings modify URL-of-destination
```

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 conectividade 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 conectividade, 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 refletos 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
Group Cluster Node          Configuration  DR
                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
Group Cluster Node      Configuration  DR
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 interruptor 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  
Group Cluster Node Configuration State DR  
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

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 conectada a fontes de alimentação separadas. Se ambas as PSUs estiverem conectadas 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 conectividade 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 interruptor 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 interruptor.

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
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
```

Vserver	Type	Subtype	Admin State	Operational State	Root 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
-----
-----

```



```

    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::> vservers show -type data

cluster_A::> vservers 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 "ressincronizando", 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 conectividade 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 conectado 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 impacto 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 conectadas 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](#)

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

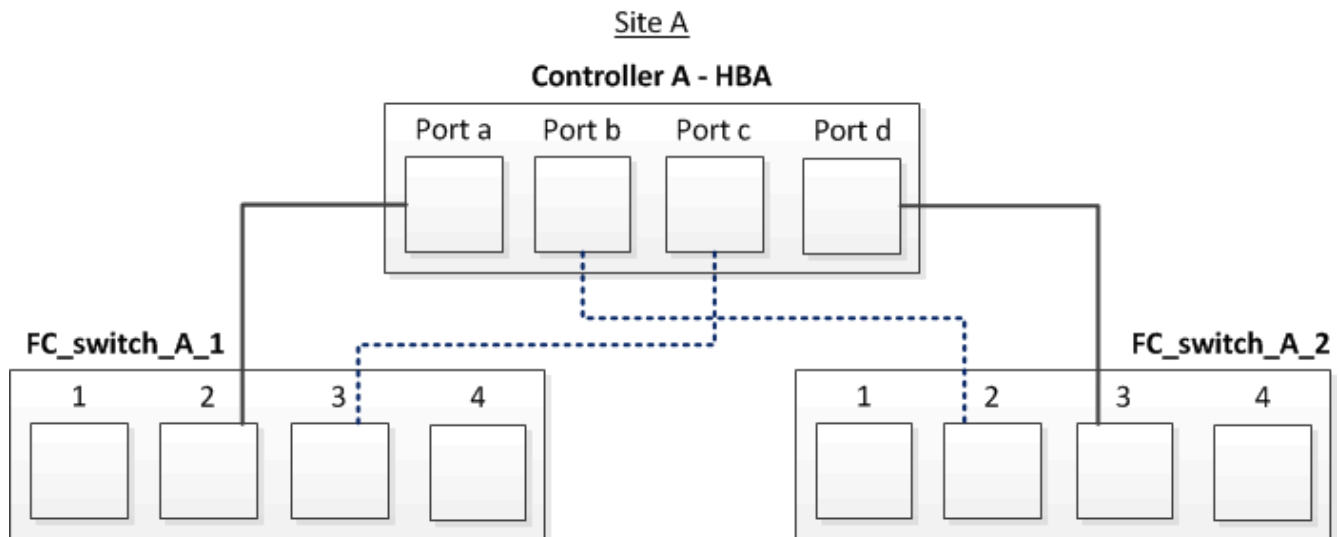
- Você deve repetir esta tarefa para cada controlador em ambos os sites do MetroCluster.
- Se você planeja usar discos além de LUNs de storage na configuração do MetroCluster, use as portas HBA e as portas de switch especificadas para configuração com discos.
 - ["Atribuições de portas para switches 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 conectadas 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

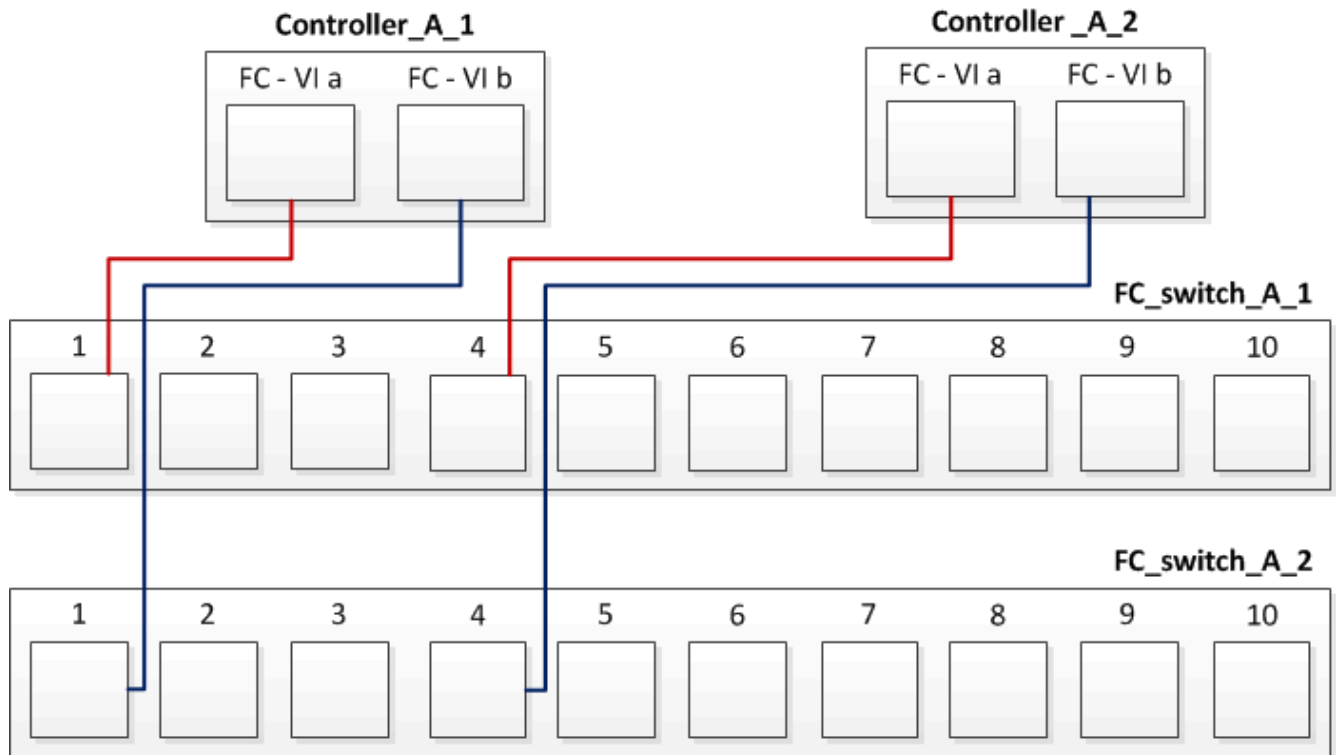
- Você deve repetir esta tarefa para cada controlador em ambos os sites do MetroCluster.
- Se você planeja usar discos além de LUNs de storage na configuração do MetroCluster, use as portas HBA e as portas de switch especificadas para configuração com discos.
 - ["Atribuições de portas para switches 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:

Site A

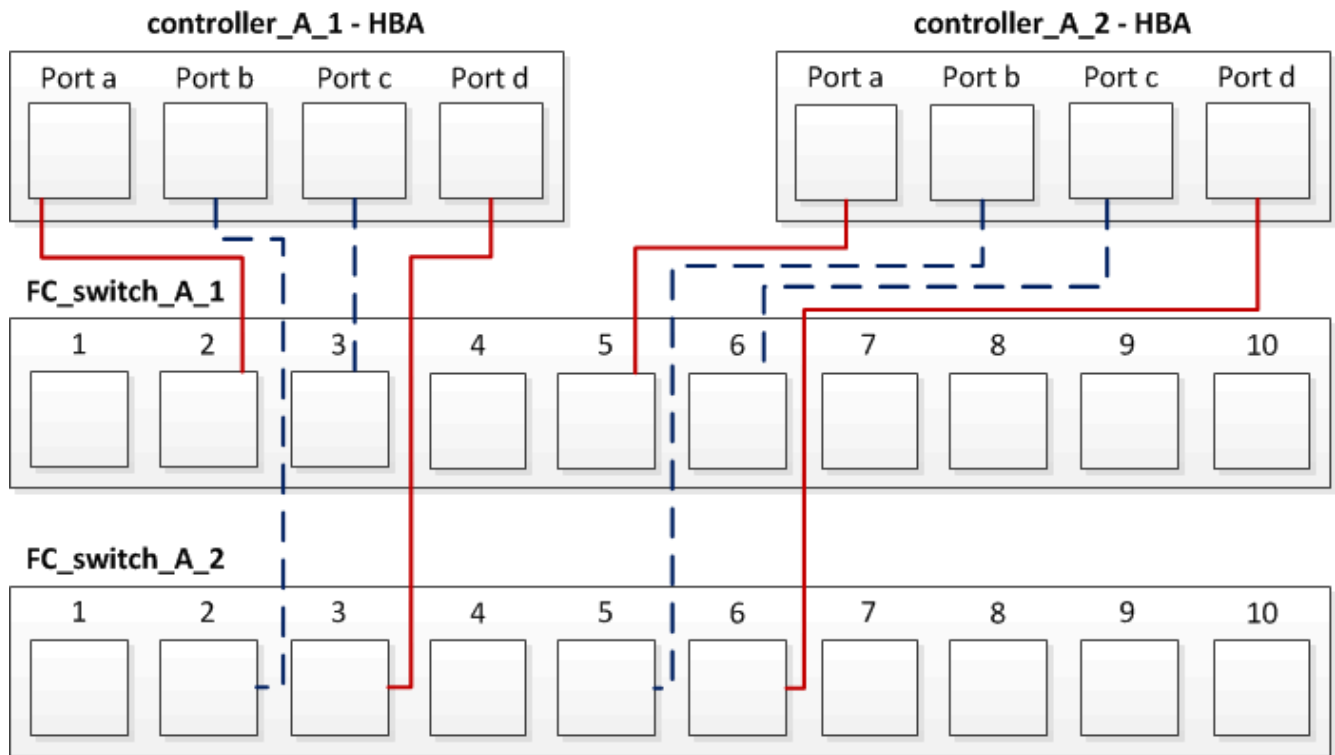


2. Execute o cabeamento de controlador para switch em ambos os locais do MetroCluster.

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 conectadas a switches FC alternativos.

O exemplo a seguir mostra as conexões entre as portas HBA e as portas do switch no local A:

Site 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. Conecte 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 interruptor	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 I	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 conectividade 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 conectividade de rede é de 1 GbE.

Passo

1. Identifique e faça o cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm conectividade 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 conectar 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"](#)

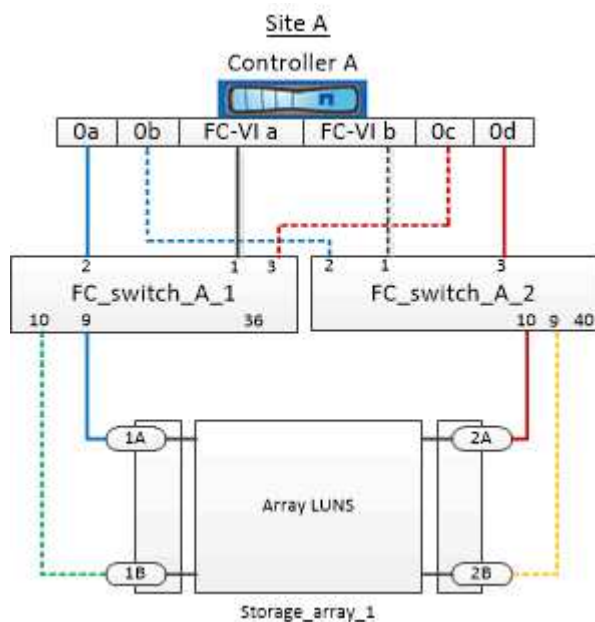
"Exemplo de cabeamento de portas de storage array para switches FC em uma configuração de MetroCluster de quatro nós"

"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 conectada 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 conectadas 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.

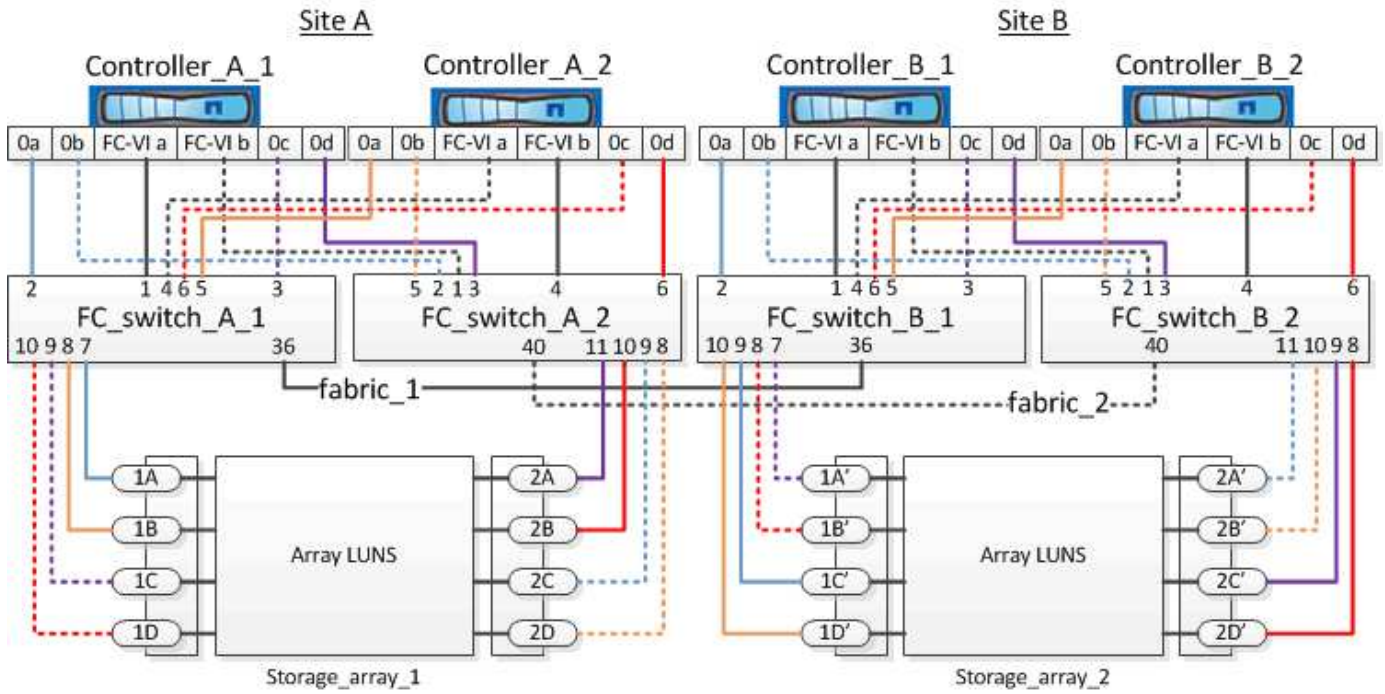
A tabela a seguir lista as conexões entre as portas do storage array e os switches FC para a ilustração MetroCluster de exemplo:

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 conectados. 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"](#)

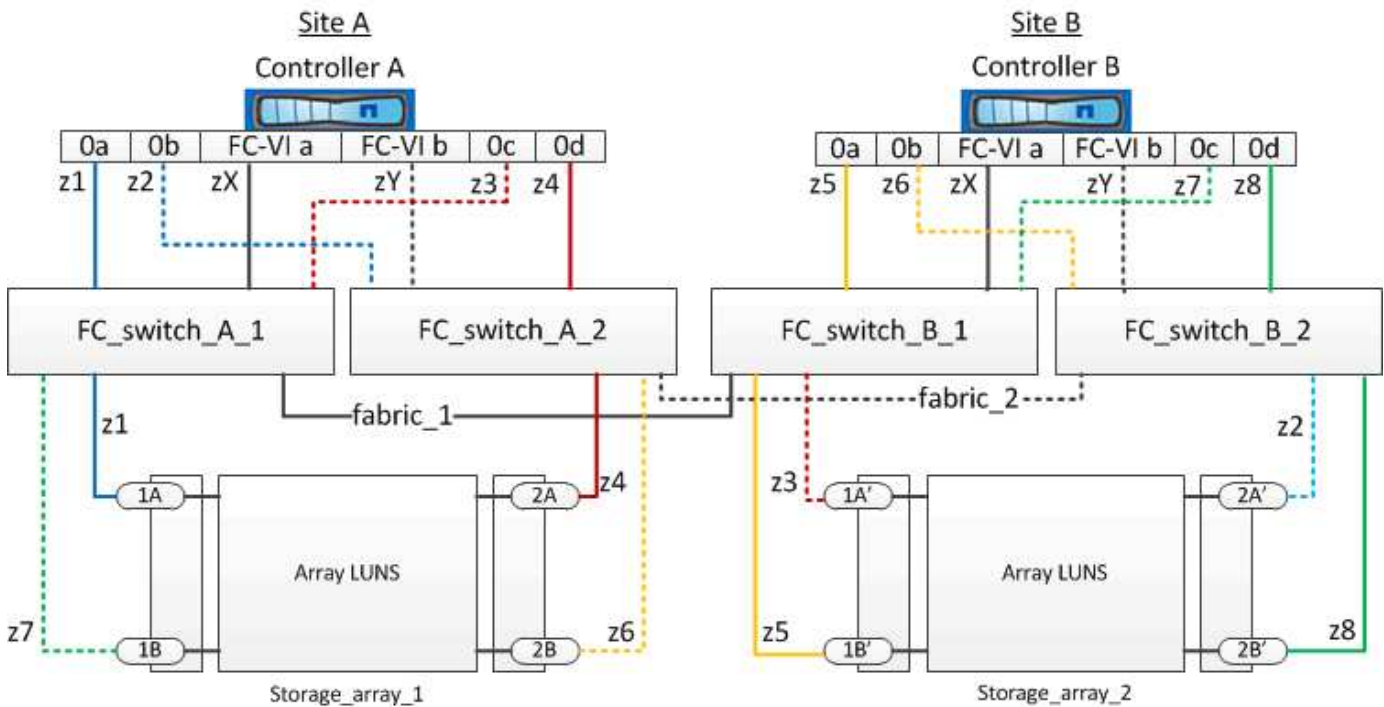
["Exemplo de zoneamento de switch em uma configuração de MetroCluster de quatro nós com LUNs de array"](#)

["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 conectados. 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 conectada 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 respectivas 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 conectados. 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"](#)

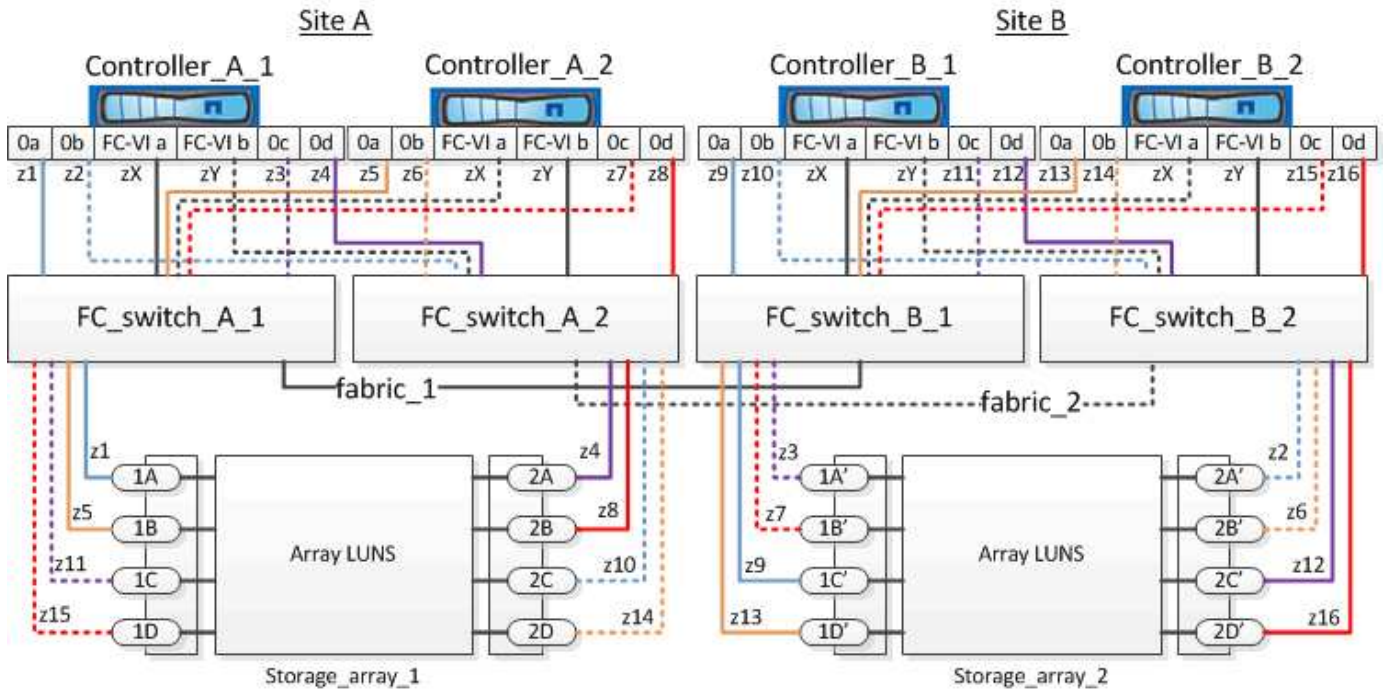
- Ao usar o zoneamento de switch em uma configuração do MetroCluster com LUNs de array, você deve garantir que certos requisitos básicos sejam seguidos.

["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 conectados. 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 respectivas 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 conectados. 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 conectado 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 detecta 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      600604803436313237643666
      3  switch0:5.183L33  SYMMETRIX  EMC        658.3 GB  local    (root)
Block      600604803436316263613066
      4  switch0:7.183L0   SYMMETRIX  EMC        173.6 GB  local
Block      600604803436313261356235
      5  switch0:7.183L2   SYMMETRIX  EMC        173.6 GB  local
Block      600604803436313438396431
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:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Verifique se as portas estão desativadas:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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 conectividade 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 conectados 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 conetada 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 conetada 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	<ul style="list-style-type: none"> • Se você estiver configurando uma implantação <i>new</i> MetroCluster com discos e LUNs de array, será necessário criar o agregado raiz em discos nativos. <p>Ao fazer isso, certifique-se de que <i> pelo menos um </i> compartimento de disco (com 24 unidades de disco) esteja configurado em cada um dos sites.</p> <ul style="list-style-type: none"> • Se você estiver adicionando discos nativos a uma configuração <i> existente </i> MetroCluster que use LUNs de array, o agregado raiz poderá permanecer em um LUN de array.
Uso de switches e pontes FC para SAS	<p>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.</p> <p>Você precisa usar os mesmos switches para se conectar aos storage arrays e às pontes FC para SAS.</p>
Usando portas do iniciador FC	<p>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.</p> <p>Um mínimo de oito portas de iniciador é necessário para conectar um sistema ONTAP a discos e LUNs de array.</p>

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 conectados. 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"

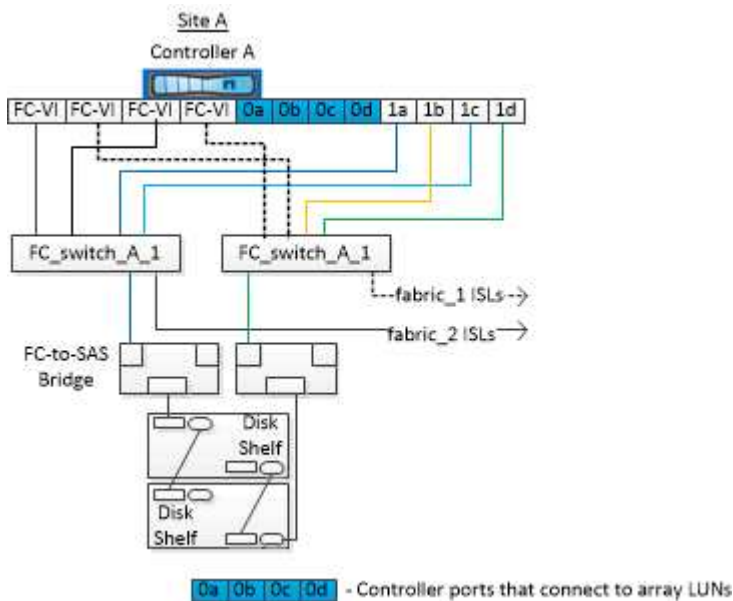
- "NetApp Hardware Universe"

Exemplo de uma configuração de MetroCluster conectada à malha de dois nós com discos e LUNs de array

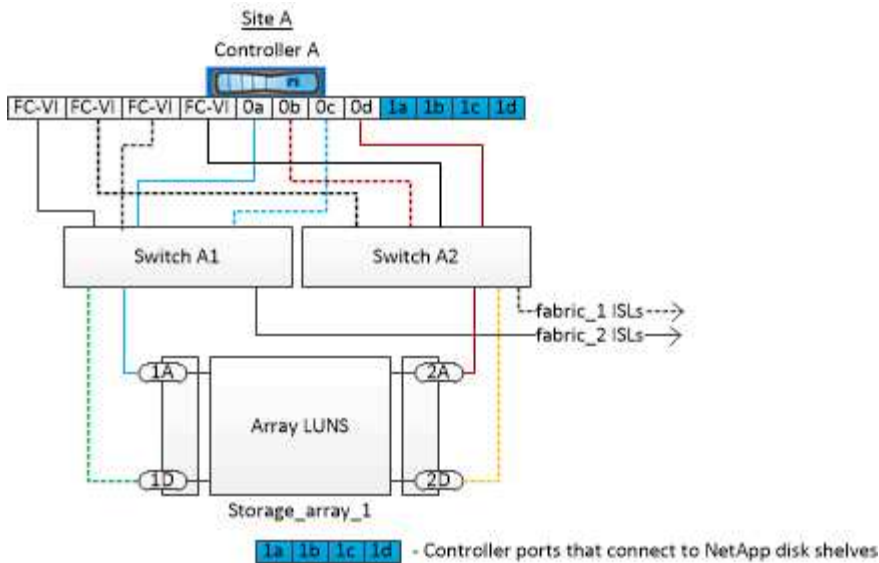
Para configurar uma configuração de MetroCluster com conexão de malha de dois nós com discos nativos e LUNs de array, é necessário usar pontes FC para SAS para conectar os sistemas ONTAP aos compartimentos de disco por meio dos switches FC. É possível conectar LUNs de array por meio dos switches FC aos 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 conectividade com discos por meio das pontes FC-para-SAS:



Na ilustração a seguir mostrando a conectividade entre sistemas ONTAP e LUNs de array, as portas HBA 0a a 0d são usadas para conectividade com LUNs de storage porque as portas 1a a 1D são usadas para conectividade com discos:



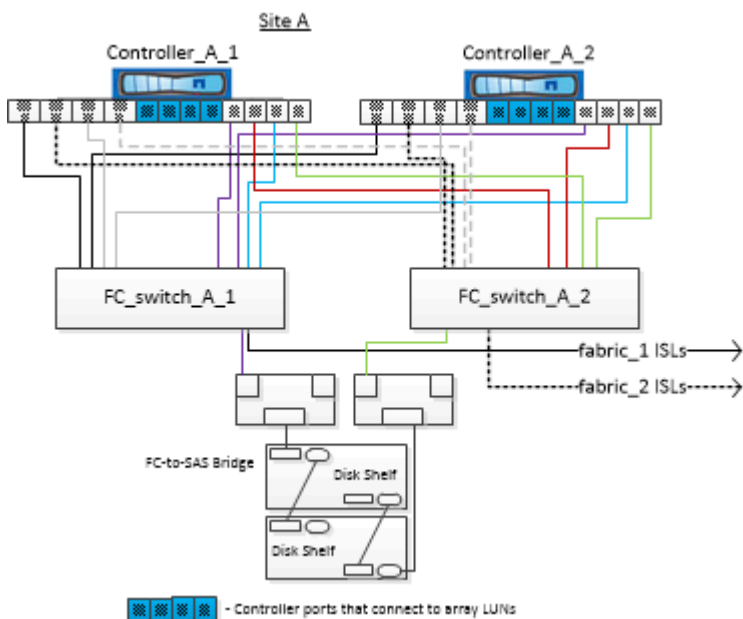
Exemplo de uma configuração de MetroCluster de quatro nós com discos e LUNs de array

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.

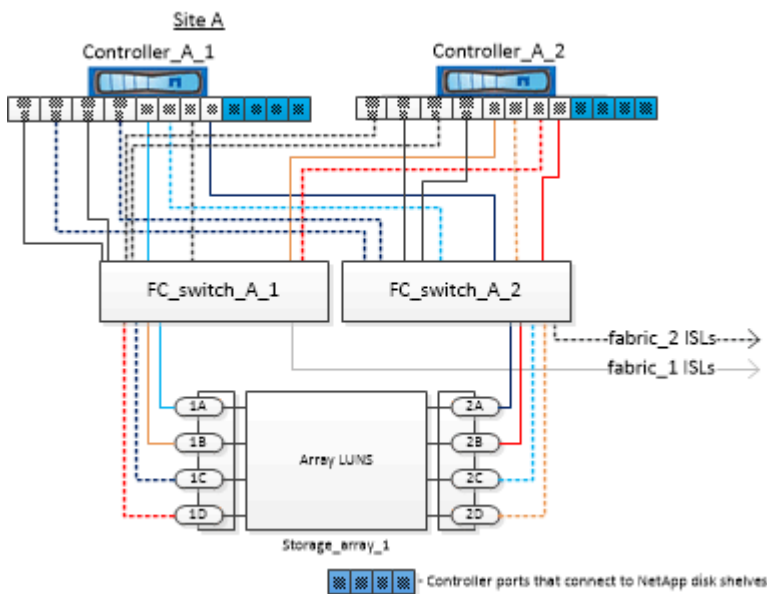
É necessário um mínimo de oito portas de iniciador para que um sistema ONTAP se conecte a discos nativos e LUNs de storage.

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 conectividade com discos por meio das pontes FC-para-SAS:



Na ilustração a seguir, que mostra a conectividade entre sistemas ONTAP e LUNs de storage, as portas HBA 0a a 0d são usadas para conectividade com LUNs de storage porque as portas 1a a 1d são usadas para conectividade 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 conectados, 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 impacto 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
Name      Subnet          Broadcast
-----  -
Domain    Gateway
-----  -
-----  -
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
Name      Subnet          Broadcast
-----  -
Domain    Gateway
-----  -
-----  -
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.

<p>Identificação da porta</p>	<p>O ONTAP identifica as portas de destino FC conectadas no cluster de DR.</p>	<p>As portas no cluster de DR que estão no mesmo espaço IPspace que o LIF de origem são selecionadas para uma verificação de acessibilidade.</p> <p>Se não houver portas no cluster de DR no mesmo IPspace, o LIF não pode ser colocado.</p> <p>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.</p>
<p>Verificação de acessibilidade</p>	<p>A acessibilidade é determinada verificando a conectividade da malha de origem WWN nas portas do cluster de DR.</p> <p>Se a mesma malha não estiver presente no local de DR, o LIF será colocado em uma porta aleatória no parceiro de DR.</p>	<p>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.</p> <p>Para que as verificações de acessibilidade sejam bem-sucedidas, os broadcasts ARP devem ser permitidos entre os dois clusters.</p> <p>Cada porta que recebe uma resposta do LIF de origem será marcada como possível para o posicionamento.</p>

<p>Seleção da porta</p>	<p>O ONTAP categoriza as portas com base em atributos como tipo e velocidade do adaptador e, em seguida, seleciona as portas com atributos correspondentes.</p> <p>Se nenhuma porta com atributos correspondentes for encontrada, o LIF será colocado em uma porta conetada aleatória no parceiro DR.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Colocação de LIF</p>	<p>A partir das portas alcançáveis, o ONTAP seleciona a porta menos carregada para colocação.</p>	<p>A partir das portas selecionadas, o ONTAP seleciona a porta menos carregada para colocação.</p>

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

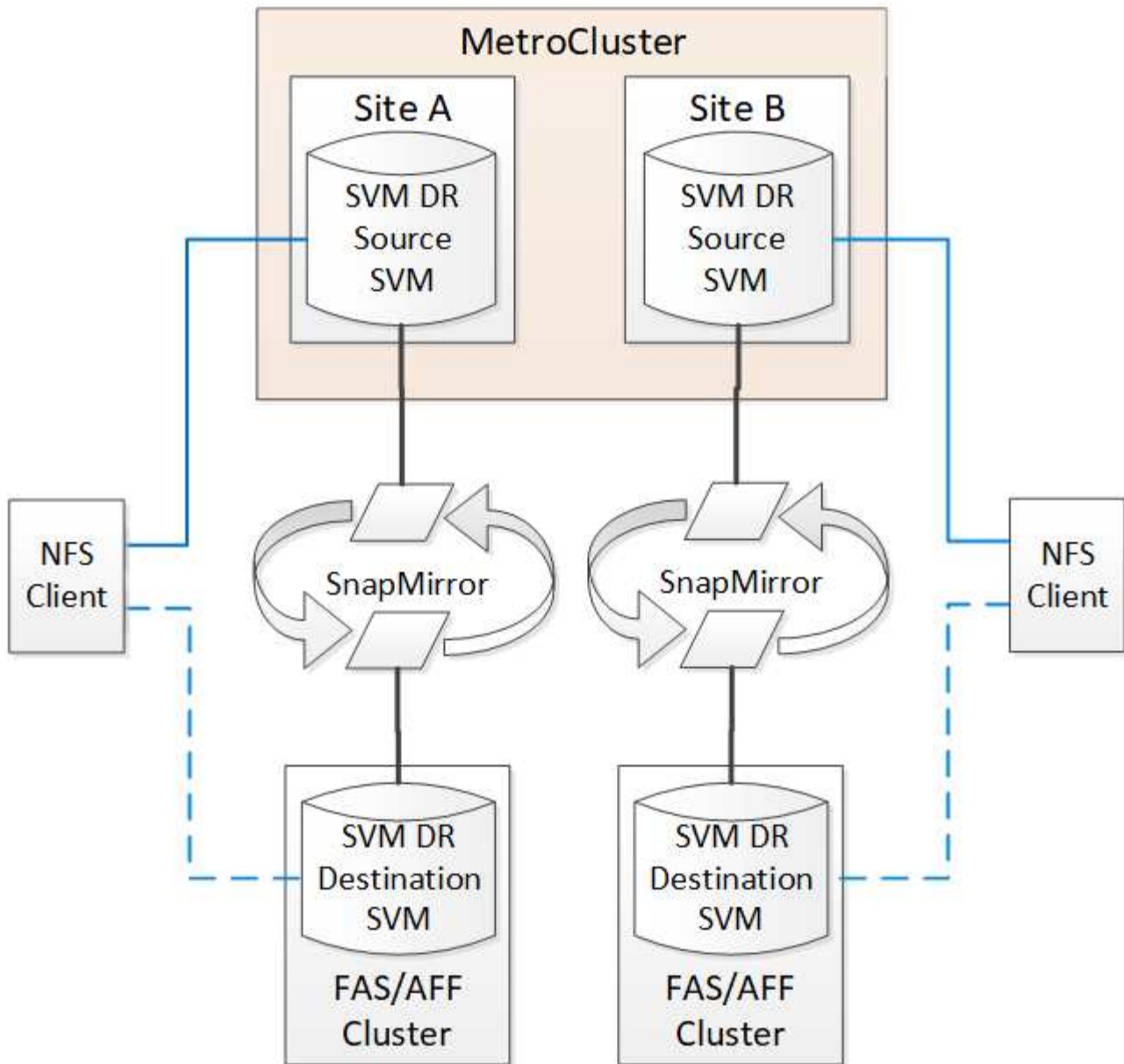
O sistema não permite a criação de novos volumes no agregado raiz (um agregado com uma política de HA do CFO) de um nó em uma configuração do MetroCluster.

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.



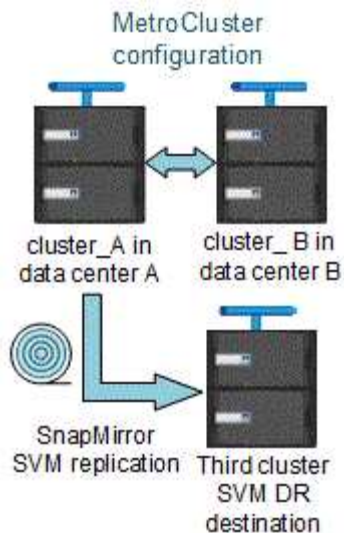
Você deve estar ciente dos seguintes requisitos e limitações de uso de SVMs com recuperação de desastres do SnapMirror:

- 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.

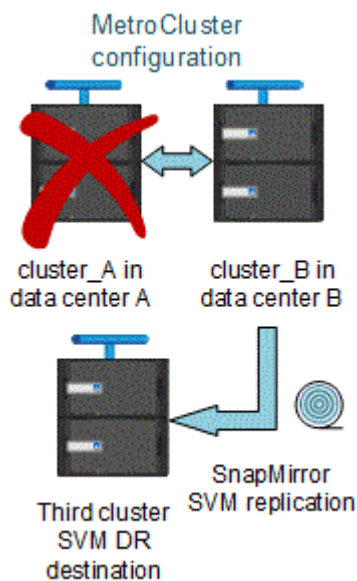
- Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online.

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.

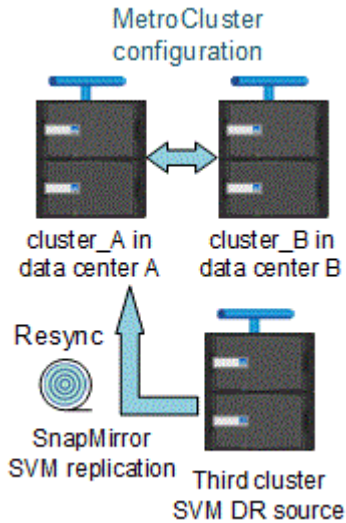
No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas do SVM DR serão bem-sucedidas.

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 resincronização, 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 resincronização

Switchovers não planejados que ocorrem durante a resincronização interromperão a transferência de resincronização. 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 resincronização) 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 switchover após um switchover não planejado durante a resincronização

Para executar com sucesso o processo de switchover, a relação de resincronização deve ser quebrada e excluída. O switchover 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"	<ul style="list-style-type: none">• Todas as informações do MetroCluster
"Arquitetura e Design de soluções da NetApp MetroCluster, TR-4705"	<ul style="list-style-type: none">• 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"	<ul style="list-style-type: none">• 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"	<ul style="list-style-type: none">• 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"	<ul style="list-style-type: none">• Arquitetura IP do MetroCluster• Fazer o cabeamento da configuração• Configurando o MetroCluster no ONTAP
"Gerenciamento de MetroCluster e recuperação de desastres"	<ul style="list-style-type: none">• Compreender a configuração do MetroCluster• Switchover, cura e switchback• Recuperação de desastres

<p>"Mantenha os componentes do MetroCluster"</p>	<ul style="list-style-type: none"> • 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 conectada 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.
<p>"Transição do MetroCluster FC para o MetroCluster IP"</p> <p>"Guia de atualização e expansão do MetroCluster"</p>	<ul style="list-style-type: none"> • 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
<p>"Instalação e configuração do software MetroCluster Tiebreaker"</p>	<ul style="list-style-type: none"> • Monitoramento da configuração do MetroCluster com o software tiebreaker da MetroCluster
<p>Documentação do consultor digital da Active IQ</p> <p>"Documentação do NetApp: Guias de produto e recursos"</p>	<ul style="list-style-type: none"> • Monitoramento da configuração e do desempenho do MetroCluster
<p>"Transição baseada em cópia"</p>	<ul style="list-style-type: none"> • Transição de dados de sistemas de storage 7-Mode para sistemas de armazenamento em cluster
<p>"Conceitos de ONTAP"</p>	<ul style="list-style-type: none"> • Como os agregados espelhados funcionam

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.