



Instale uma configuração Stretch MetroCluster

ONTAP MetroCluster

NetApp
January 10, 2025

Índice

Instale uma configuração Stretch MetroCluster	1
Visão geral	1
Prepare-se para a instalação do MetroCluster	1
Escolhendo o procedimento de instalação correto para sua configuração	6
Cabo uma configuração Stretch MetroCluster de dois nós conetada a SAS	7
Cable uma configuração Stretch MetroCluster com conexão em ponte de dois nós	13
Configurando o software MetroCluster no ONTAP	36
Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster	75
Testando a configuração do MetroCluster	78
Conexões em configurações Stretch MetroCluster com LUNs de array	96
Considerações ao remover configurações do MetroCluster	100
Como usar o Active IQ Unified Manager e o Gerenciador de sistemas ONTAP para configuração e monitoramento adicionais	100
Considerações ao usar o ONTAP em uma configuração do MetroCluster	101
Transição de uma configuração MetroCluster elástica para uma configuração de malha	111
Onde encontrar informações adicionais	112

Instale uma configuração Stretch MetroCluster

Visão geral

Para instalar sua configuração Stretch MetroCluster, você deve executar vários procedimentos na ordem correta.

- ["Prepare-se para a instalação e entenda todos os requisitos"](#)
- ["Escolha o procedimento de instalação correto"](#)
- Faça o cabo dos componentes
 - ["Configuração de conexão SAS de dois nós"](#)
 - ["Configuração de conexão em ponte de dois nós"](#)
- ["Configure o software"](#)
- ["Teste a configuração"](#)

Prepare-se para a instalação do MetroCluster

Diferenças entre as configurações do ONTAP MetroCluster

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

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

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

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

Importante

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

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

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

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

A400.

As configurações de plataforma compatíveis estão listadas no ["NetApp Hardware Universe"](#).

Peering de clusters

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

Informações relacionadas

["Configuração expressa de peering de cluster e SVM"](#)

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar que a 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 ao usar agregados sem espelhamento

Considerações ao usar agregados sem espelhamento

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

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

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

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

Considerações para agregados sem espelhamento e namespaces hierárquicos

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

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

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

Considerações para agregados sem espelhamento e SVMs

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

Considerações para agregados sem espelhamento e SAN

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

Uso de firewall em sites da MetroCluster

Considerações sobre o uso de firewall em sites da MetroCluster

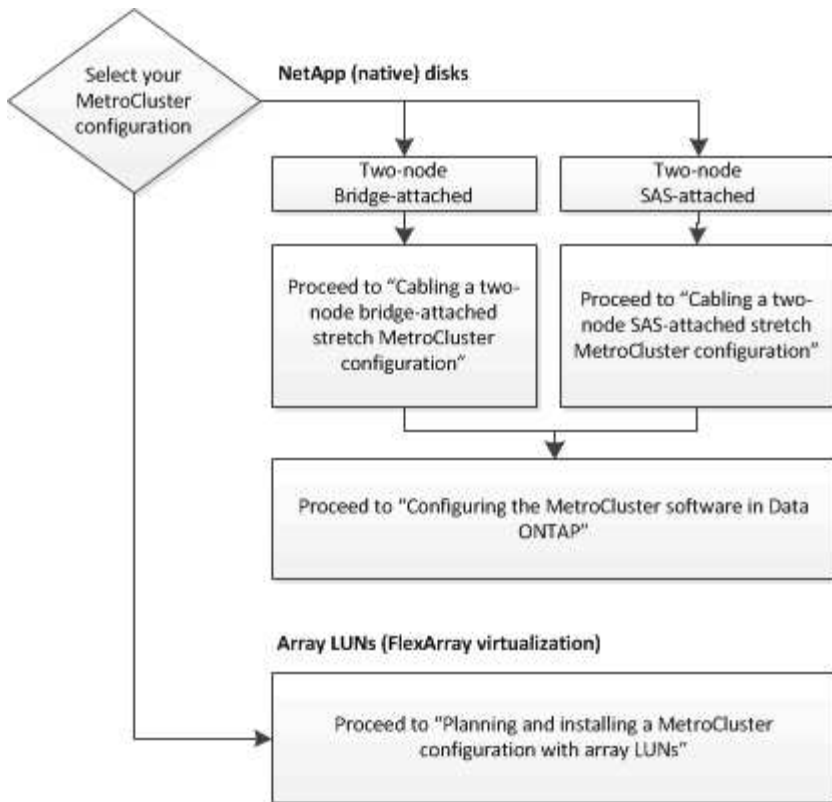
Se você estiver usando um firewall em um site da MetroCluster, você deverá garantir o acesso às portas necessárias.

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

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

Escolhendo o procedimento de instalação correto para sua configuração

Você deve escolher o procedimento de instalação correto com base no uso de LUNs FlexArray e na forma como os controladores de storage se conectam às gavetas de storage.

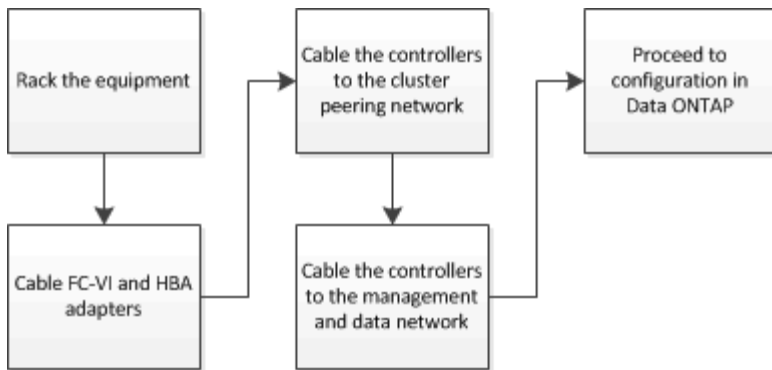


Para este tipo de instalação...	Utilize estes procedimentos...
Configuração elástica de dois nós com pontes FC para SAS	<ol style="list-style-type: none"> 1. "Cabeamento de uma configuração Stretch MetroCluster de dois nós conetada em ponte" 2. "Configurando o software MetroCluster no ONTAP"
Configuração elástica de dois nós com cabeamento SAS de conexão direta	<ol style="list-style-type: none"> 1. "Cabeamento de uma configuração Stretch MetroCluster com conexão SAS de dois nós" 2. "Configurando o software MetroCluster no ONTAP"
Instalação com LUNs de array	"Conexões em configurações Stretch MetroCluster com LUNs de array"

Cabo uma configuração Stretch MetroCluster de dois nós conetada a SAS

Cabeamento de uma configuração Stretch MetroCluster com conexão SAS de dois nós

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



Partes de uma configuração Stretch MetroCluster de dois nós conectada a SAS

A configuração de conexão SAS com MetroCluster de dois nós requer várias peças, incluindo dois clusters de nó único nos quais os controladores de storage são diretamente conectados ao storage usando cabos SAS.

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

- Controladores de storage

Os controladores de storage se conectam diretamente ao storage usando cabos SAS.

Cada controlador de storage é configurado como parceiro de recuperação de desastres para um controlador de storage no local do parceiro.

- Cabos SAS de cobre podem ser usados para distâncias mais curtas.
- Os cabos SAS óticos podem ser usados para distâncias mais longas.



Em sistemas que usam LUNs de array e-Series, os controladores de storage podem ser diretamente conectados aos storage arrays e-Series. Para outros LUNs de array, são necessárias conexões por meio de switches FC.

"Ferramenta de Matriz de interoperabilidade do NetApp"

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

- Rede de peering de cluster

A rede de peering de cluster fornece conectividade para espelhamento da configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.

Componentes de hardware MetroCluster necessários e diretrizes de nomenclatura para configurações de stretch com conexão SAS de dois nós

A configuração do MetroCluster requer uma variedade de componentes de hardware. Para conveniência e clareza, os nomes padrão dos componentes são usados em toda a

documentação do MetroCluster. Um site é referido como Site A e o outro site é referido como Site B.

Software e hardware suportados

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

["NetApp Hardware Universe"](#)

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

Redundância de hardware na configuração MetroCluster

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

Dois clusters ONTAP de nó único

A configuração Stretch MetroCluster conectada ao SAS requer dois clusters ONTAP de nó único.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Dois módulos de controlador de armazenamento

A configuração Stretch MetroCluster conectada a SAS requer dois módulos de controlador de armazenamento.

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

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

- Portas FC-VI integradas
- Uma placa FC-VI no slot 1

Uma combinação de um módulo de controladora que usa portas FC-VI integradas e outra que usa uma placa FC-VI complementar não é compatível. Por exemplo, se um nó usar a configuração FC-VI integrada, todos os outros nós do grupo de DR também precisarão usar a configuração FC-VI integrada.

Nomes de exemplo:

- Local A: Controller_A_1

- Local B: Controller_B_1

Pelo menos quatro compartimentos de disco SAS (recomendado)

A configuração Stretch MetroCluster conectada a SAS requer pelo menos duas gavetas de disco SAS. Recomenda-se quatro compartimentos de disco SAS.

Duas gavetas são recomendadas em cada local para permitir a propriedade de disco por compartimento. Há suporte para um mínimo de uma prateleira em cada local.

Nomes de exemplo:

- Local A:
 - shelf_A_1_1
 - shelf_A_1_2
- Local B:
 - shelf_B_1_1
 - shelf_B_1_2

Misturando módulos IOM12 e IOM 6 em uma pilha

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

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

Instale e faça o cabo dos componentes MetroCluster para configurações de alongamento de dois nós conectadas a SAS

Instalação e cabeamento de componentes MetroCluster para configurações de alongamento de dois nós conectadas a SAS

Os controladores de storage devem ser cabeados para a Mídia de storage e entre si. Os controladores de storage também devem ser cabeados para a rede de dados e gerenciamento.

Antes de iniciar qualquer procedimento neste documento

Os seguintes requisitos gerais devem ser atendidos antes de concluir esta tarefa:

- Antes da instalação, você deve se familiarizar com as considerações e as práticas recomendadas para instalação e cabeamento de compartimentos de disco para o modelo de compartimento de disco.
- Todos os componentes do MetroCluster devem ser suportados.

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

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

Sobre esta tarefa

- Os termos nó e controlador são usados de forma intercambiável.

Colocar em pilha os componentes de hardware

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

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

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

A quantidade de espaço em rack necessária depende do modelo de plataforma das controladoras de storage, dos tipos de switch e do número de stacks de compartimento de disco na configuração.

2. Utilizando práticas de oficina padrão para trabalhar com equipamentos elétricos, certifique-se de que está devidamente ligado à terra.
3. Instale os controladores de armazenamento no rack ou gabinete.

["Documentação dos sistemas de hardware da ONTAP"](#)

4. Instale as gavetas de disco, encadeie em série as gavetas de disco em cada pilha, ligue-as e defina as IDs de gaveta.

Consulte o guia apropriado para o modelo do compartimento de disco para obter informações sobre prateleiras de disco em encadeamento em série e sobre a configuração de IDs de gaveta.



As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais). Ao definir manualmente as IDs de gaveta, você deve desligar o compartimento de disco.

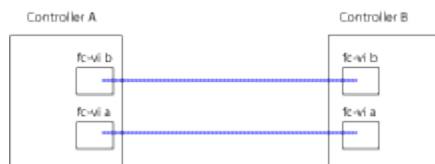
Fazer o cabeamento das controladoras umas para as outras e das gavetas de storage

Os adaptadores FC-VI da controladora devem ser cabeados diretamente entre si. As portas SAS da controladora devem ser cabeadas para as stacks de storage remoto e local.

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

Passos

1. Cable as portas FC-VI.

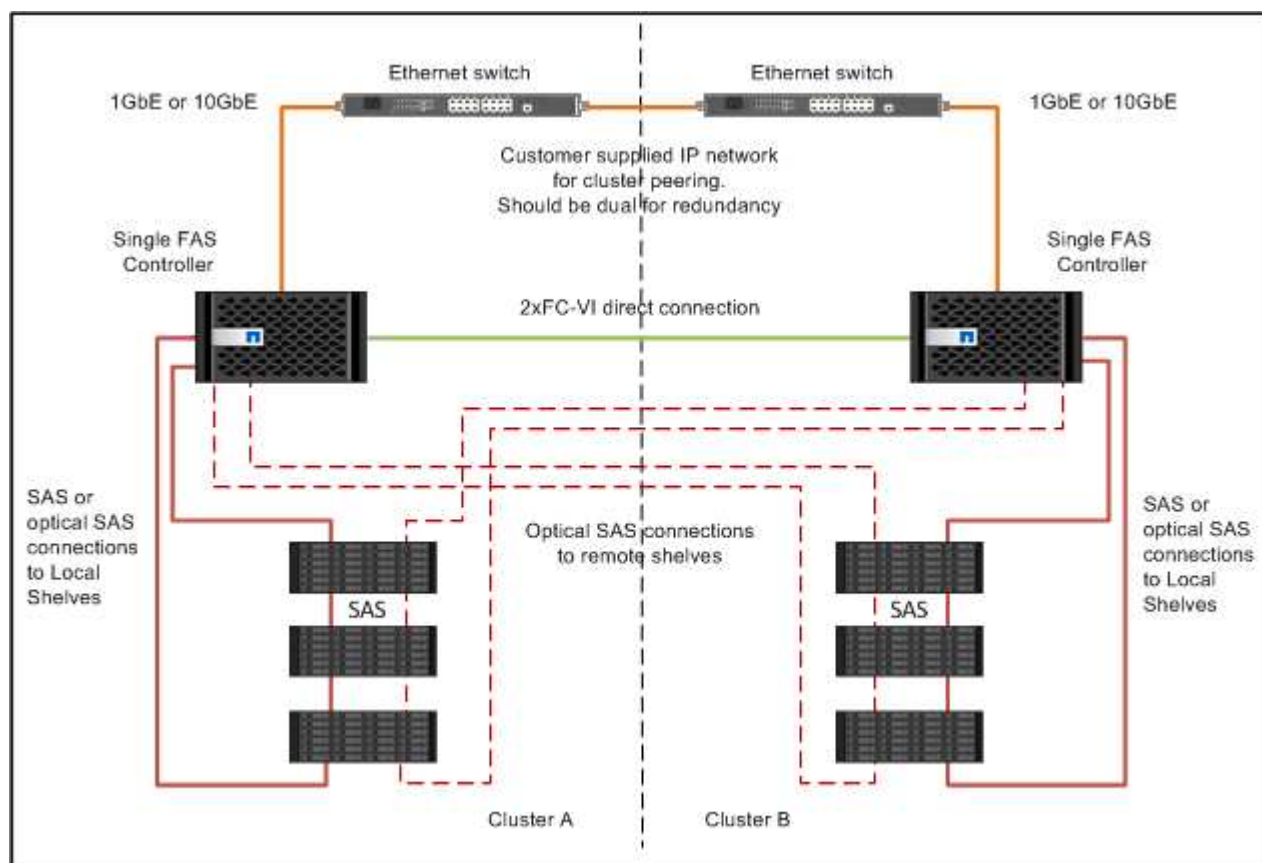


A ilustração acima é uma conexão de cabo representativa típica. As portas FC-VI específicas variam de acordo com o módulo do controlador.

- Os módulos de controladora FAS8200 e AFF A300 podem ser solicitados com uma das duas opções de conectividade FC-VI:
 - As portas integradas 0e e 0f são configuradas no modo FC-VI.
 - As portas 1a e 1b em uma placa FC-VI entram no slot 1.
- Os módulos dos controladores de sistemas de storage AFF A700 e FAS9000 usam quatro portas FC-VI cada uma.
- Os módulos de controladora do sistema de storage AFF A400 e FAS8300 usam as portas FC-VI 2a e 2b.

2. Faça o cabo das portas SAS.

A ilustração a seguir mostra as conexões. O uso da porta pode ser diferente dependendo das portas SAS e FC-VI disponíveis no módulo da controladora.



Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de cluster para que eles tenham conectividade com o cluster no local do parceiro.

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

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

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

Passos

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm 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 uma taxa de transferência mais alta para o tráfego de peering de cluster.

["Configuração expressa de peering de cluster e SVM"](#)

Cabeamento das conexões de dados e gerenciamento

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

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

Pode ligar as portas de gestão do controlador e do comutador de cluster a comutadores existentes na rede. Além disso, você pode conectar o controlador a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passos

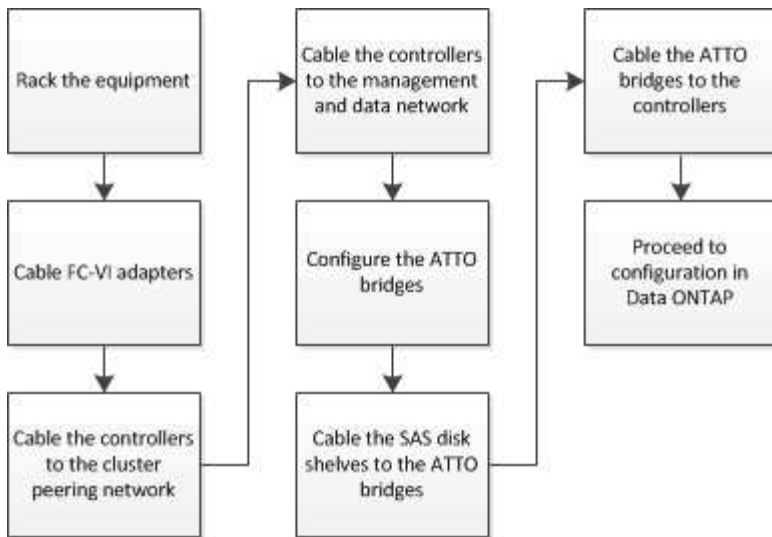
1. Faça o cabeamento das portas de gerenciamento e dados do controlador para as redes de gerenciamento e dados no local.

["Documentação dos sistemas de hardware da ONTAP"](#)

Cable uma configuração Stretch MetroCluster com conexão em ponte de dois nós

Cabeamento de uma configuração Stretch MetroCluster de dois nós conectada em ponte

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



Partes de uma configuração Stretch MetroCluster de dois nós conectada em ponte

Ao Planejar sua configuração do MetroCluster, você deve entender as partes da configuração e como elas funcionam juntas.

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

- Controladores de storage

As controladoras de storage não são conectadas diretamente ao storage, mas conectadas a pontes FC para SAS. Os controladores de storage são conectados por cabos FC entre os adaptadores FC-VI de cada controlador.

Cada controlador de storage é configurado como parceiro de recuperação de desastres para um controlador de storage no local do parceiro.

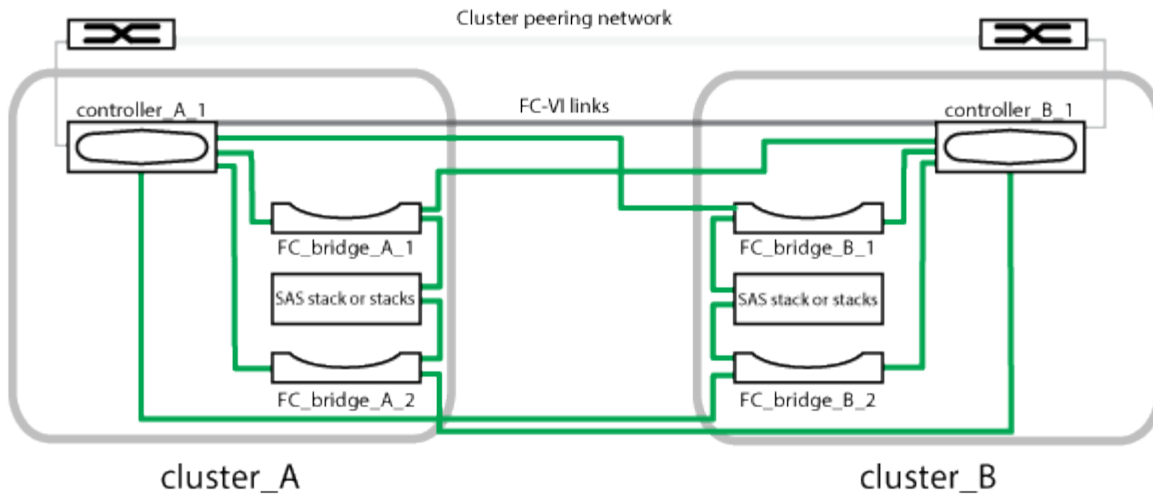
- Pontes FC para SAS

As pontes FC para SAS conectam as stacks de storage SAS às portas iniciadores de FC nas controladoras, fornecendo uma ponte entre os dois protocolos.

- Rede de peering de cluster

A rede de peering de cluster fornece conectividade para espelhamento da configuração de máquina virtual de storage (SVM). A configuração de todos os SVMs em um cluster é espelhada para o cluster de parceiros.

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



- A configuração consiste em dois clusters de nó único.
- Cada local tem uma ou mais pilhas de storage SAS.



Gavetas SAS em configurações MetroCluster não são compatíveis com cabeamento ACP.

São suportadas stacks de armazenamento adicionais, mas apenas uma é mostrada em cada local.

Componentes de hardware necessários da MetroCluster e convenções de nomenclatura para configurações de stretch anexadas a ponte de dois nós

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

Software e hardware suportados

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

["NetApp Hardware Universe"](#)

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

Redundância de hardware na configuração MetroCluster

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

Requisito para dois clusters ONTAP de nó único

A configuração Stretch MetroCluster conectada a ponte requer dois clusters ONTAP de nó único.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Requisito para dois módulos de controlador de armazenamento

A configuração Stretch MetroCluster conectada em ponte requer dois módulos de controlador de armazenamento.

Os controladores devem atender aos seguintes requisitos:

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

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

- Portas FC-VI integradas
- Uma placa FC-VI no slot 1

Uma combinação de um módulo de controladora que usa portas FC-VI integradas e outra que usa uma placa FC-VI complementar não é compatível. Por exemplo, se um nó usar a configuração FC-VI integrada, todos os outros nós do grupo de DR também precisarão usar a configuração FC-VI integrada.

Nomes de exemplo:

- Local A: Controller_A_1
- Local B: Controller_B_1

Requisito para pontes FC para SAS

A configuração Stretch MetroCluster conectada em ponte requer duas ou mais pontes FC para SAS em cada local.

Essas pontes conectam os compartimentos de disco SAS aos módulos da controladora.



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

- As pontes FibreBridge 7600N e 7500N suportam até quatro stacks SAS.
- Cada stack pode usar modelos diferentes de IOM, mas todas as gavetas de uma stack precisam usar o mesmo modelo.

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

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

Os nomes sugeridos usados como exemplos neste procedimento identificam o módulo do controlador ao qual a ponte se conecta e a porta.

Nomes de exemplo:

- Local A:
 - `ponte_A_1_port-number`
 - `ponte_A_2_port-number`
- Local B:
 - `ponte_B_1_port-number`
 - `ponte_B_2_port-number`

Requisito para pelo menos quatro gavetas SAS (recomendado)

A configuração Stretch MetroCluster conectada em ponte requer pelo menos duas gavetas SAS. No entanto, duas gavetas são recomendadas em cada local para permitir a propriedade de disco por compartimento, totalizando quatro gavetas SAS.

Há suporte para um mínimo de uma prateleira em cada local.

Nomes de exemplo:

- Local A:
 - `shelf_A_1_1`
 - `shelf_A_1_2`
- Local B:
 - `shelf_B_1_1`
 - `shelf_B_1_2`

Misturando módulos IOM12 e IOM 6 em uma pilha

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

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

Planilha de coleta de informações para bridges FC-para-SAS

Antes de começar a configurar os sites do MetroCluster, você deve coletar as informações de configuração necessárias.

Local A, ponte FC-para-SAS 1 (FC_bridge_A_1a)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte se conecta ao `Controller_A_1_port-number` e `Controller_B_1_port-number`.

Local A	O seu valor
Endereço IP Bridge_A_1a	
Nome de utilizador Bridge_A_1a	
Senha Bridge_A_1a	

Local A, ponte FC-para-SAS 2 (FC_bridge_A_1b)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte se conecta ao Controller_A_1_port-number e Controller_B_1_port-number.

Local A	O seu valor
Endereço IP Bridge_A_1b	
Nome de utilizador Bridge_A_1b	
Senha Bridge_A_1b	

Local B, ponte FC-para-SAS 1 (FC_bridge_B_1a)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte conecta-se ao Controller_A_1_port-number' e Controller_B_1____port-number.

Local B	O seu valor
Endereço IP Bridge_B_1a	
Nome de utilizador Bridge_B_1a	
Bridge_B_1a Palavra-passe	

Local B, ponte FC-para-SAS 2 (FC_bridge_B_1b)

Cada stack SAS requer pelo menos duas pontes FC para SAS.

Cada ponte conecta-se ao Controller_A_1_port-number' e Controller_B_1____port-number.

Local B	O seu valor
Endereço IP Bridge_B_1b	
Nome de utilizador Bridge_B_1b	

Instale e faça o cabo dos componentes do MetroCluster

Colocar em pilha os componentes de hardware

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

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

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

O espaço em rack depende do modelo de plataforma dos controladores de storage, dos tipos de switch e do número de stacks de compartimento de disco na sua configuração.

2. Aterre-se corretamente.
3. Instale os controladores de armazenamento no rack ou gabinete.

["Documentação dos sistemas de hardware da ONTAP"](#)

4. Instale as gavetas de disco, ligue-as e defina as IDs de gaveta.
 - É necessário desligar cada compartimento de disco.
 - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
5. Instalar cada ponte FC para SAS:

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

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

Para obter mais informações e uma ilustração da instalação, consulte o *ATTO FibreBridge Installation and Operation Manual para o seu modelo de ponte*.

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



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

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

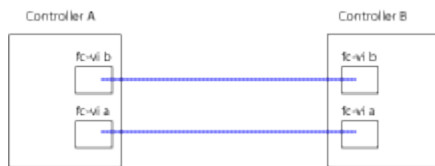
Fazer o cabeamento das controladoras umas para as outras

Os adaptadores FC-VI de cada controladora devem ser cabeados diretamente ao

parceiro.

Passos

1. Cable as portas FC-VI.



A ilustração acima é uma representação típica do cabeamento necessário. As portas FC-VI específicas variam de acordo com o módulo do controlador.

- Os módulos de controladora AFF A300 e FAS8200 podem ser solicitados com uma das duas opções de conectividade FC-VI:
 - Portas integradas 0e e 0f configuradas no modo FC-VI.
 - Portas 1a e 1b em uma placa FC-VI no slot 1.
- Os módulos dos controladores de sistemas de storage AFF A700 e FAS9000 usam quatro portas FC-VI cada uma.

Cabeamento das conexões de peering de cluster

Você deve enviar por cabo as portas do módulo do controlador usadas para peering de cluster para que eles tenham conectividade com o cluster no local do parceiro.

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

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

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

Passos

1. Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm 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 uma taxa de transferência mais alta para o tráfego de peering de cluster.

["Configuração expressa de peering de cluster e SVM"](#)

Cabeamento das conexões de dados e gerenciamento

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

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

Pode ligar as portas de gestão do controlador e do comutador de cluster a comutadores existentes na rede. Além disso, você pode conectar o controlador a novos switches de rede dedicados, como os switches de gerenciamento de cluster NetApp CN1601.

Passos

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

["Documentação dos sistemas de hardware da ONTAP"](#)

Instalar pontes FC a SAS e gavetas de disco SAS

Instale e faça o cabeamento das pontes ATTO FibreBridge e das gavetas de disco SAS quando você adicionar novo armazenamento à configuração.

Sobre esta tarefa

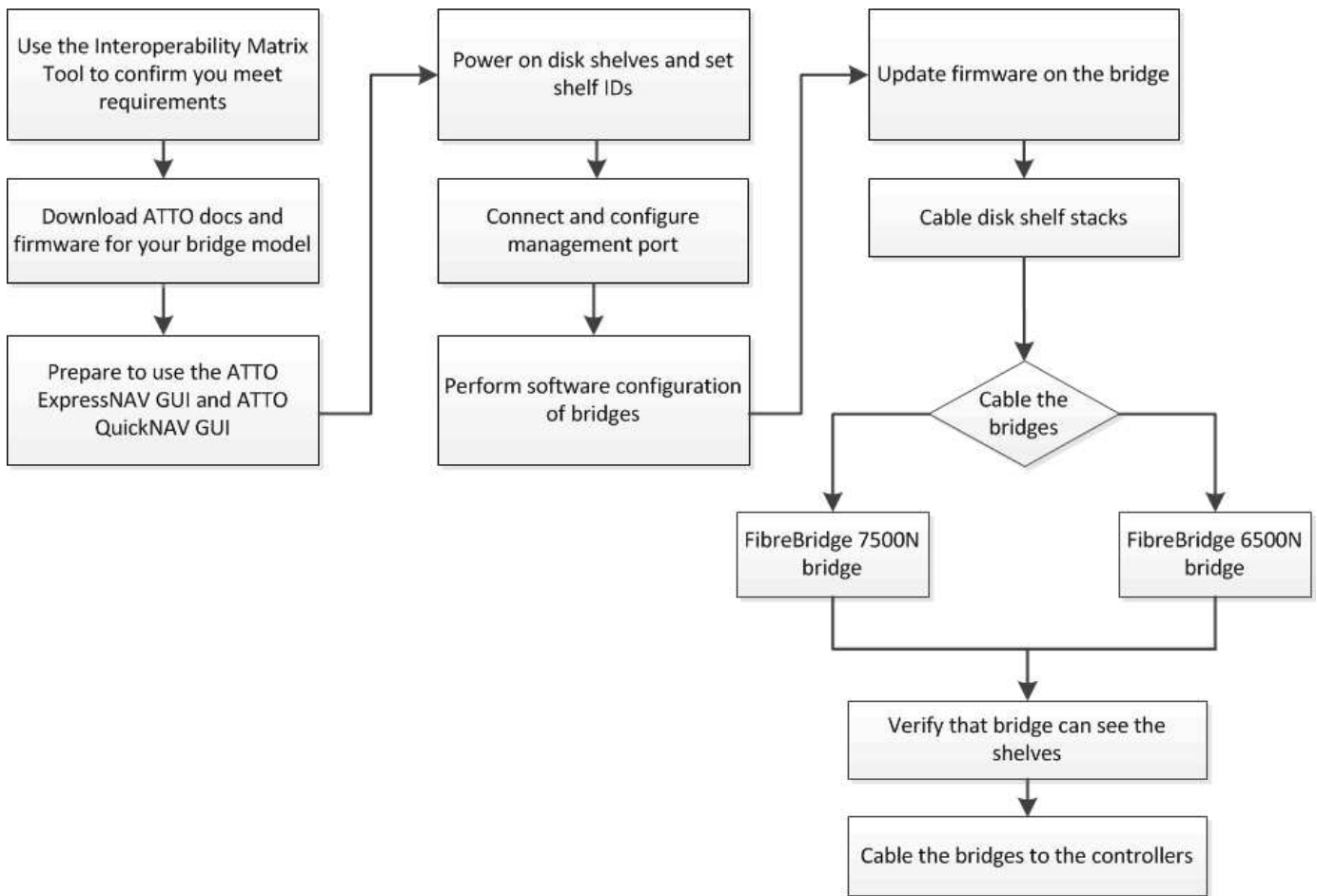
Para sistemas recebidos de fábrica, as pontes FC para SAS são pré-configuradas e não exigem configuração adicional.

Este procedimento é escrito com a suposição de que você está usando as interfaces de gerenciamento de bridge recomendadas: A GUI ATTO ExpressNAV e o utilitário ATTO Quicknav.

Você usa a GUI ATTO ExpressNAV para configurar e gerenciar uma bridge e atualizar o firmware da bridge. Você usa o utilitário ATTO Quicknav para configurar a porta 1 de gerenciamento Ethernet bridge.

Em vez disso, você pode usar outras interfaces de gerenciamento, se necessário, como uma porta serial ou Telnet para configurar e gerenciar uma ponte e configurar a porta 1 de gerenciamento Ethernet e FTP para atualizar o firmware da ponte.

Este procedimento utiliza o seguinte fluxo de trabalho:



Gerenciamento na banda das pontes FC para SAS

Começando com o ONTAP 9.5 com o FibreBridge 7500N ou 7600N bridges, *in-band Management* das bridges é suportado como uma alternativa ao gerenciamento IP das bridges. A partir do ONTAP 9.8, o gerenciamento fora da banda está obsoleto.



A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Ao usar o gerenciamento na banda, as bridges podem ser gerenciadas e monitoradas a partir da CLI do ONTAP usando a conexão FC à ponte. O acesso físico à ponte através das portas Ethernet da ponte não é necessário, reduzindo a vulnerabilidade de segurança da ponte.

A disponibilidade do gerenciamento em banda das pontes depende da versão do ONTAP:

- A partir do ONTAP 9.8, as bridges são gerenciadas por meio de conexões na banda por padrão e o gerenciamento fora da banda das bridges via SNMP é obsoleto.
- ONTAP 9.5 a 9,7: O gerenciamento na banda ou o gerenciamento SNMP fora da banda é suportado.
- Antes do ONTAP 9,5, somente o gerenciamento SNMP fora da banda é suportado.

Os comandos Bridge CLI podem ser emitidos a partir do comando ONTAP `interface storage bridge run-
cli -name <bridge_name> -command <bridge_command_name>` na interface ONTAP.



O uso do gerenciamento na banda com acesso IP desativado é recomendado para melhorar a segurança limitando a conectividade física da ponte.

Limites e regras de anexo da ponte FibreBridge 7600N e 7500N

Reveja os limites e considerações ao anexar pontes FibreBridge 7600N e 7500N.

Limites das pontes FibreBridge 7600N e 7500N

- O número máximo de unidades HDD e SSD combinadas é 240.
- O número máximo de unidades SSD é 96.
- O número máximo de SSDs por porta SAS é 48.
- O número máximo de gavetas por porta SAS é de 10.

Regras de anexo de ponte FibreBridge 7600N e 7500N

- Não misture unidades SSD e HDD na mesma porta SAS.
- Distribua as gavetas uniformemente entre as portas SAS.
- Você não deve ter DS460 gavetas na mesma porta SAS que outros tipos de gaveta (por exemplo, DS212 ou DS224 gavetas).

Exemplo de configuração

A seguir mostra um exemplo de configuração para conectar quatro gavetas DS224 com unidades SSD e seis gavetas DS224 com unidades HDD:

Porta de SAS	Compartimentos e unidades
Porta SAS A	2x DS224 gavetas com unidades SSD
Porta SAS-B	2x DS224 gavetas com unidades SSD
Porta SAS-C	3x DS224 gavetas com unidades HDD
Porta SAS-D	3x DS224 gavetas com unidades HDD

Prepare-se para a instalação

Quando estiver se preparando para instalar as bridges como parte do seu novo sistema MetroCluster, verifique se o sistema atende a certos requisitos, incluindo atender aos requisitos de configuração e configuração das bridges. Outros requisitos incluem o download dos documentos necessários, o utilitário ATTO Quicknav e o firmware da ponte.

Antes de começar

- Seu sistema já deve ser instalado em um rack se ele não foi enviado em um gabinete do sistema.
- Sua configuração deve estar usando modelos de hardware e versões de software compatíveis.

No "[Ferramenta de Matriz de interoperabilidade NetApp \(IMT\)](#)", você pode usar o campo **solução de armazenamento** para selecionar sua solução MetroCluster. Você pode usar o **Explorador de componentes** para selecionar os componentes e a versão do ONTAP para refinar sua pesquisa. Você pode selecionar **Mostrar resultados** para exibir a lista de configurações compatíveis que correspondem aos critérios.

- Cada controlador FC precisa ter uma porta FC disponível para uma ponte para se conectar a ele.

- Você deve estar familiarizado com como lidar com cabos SAS e com as considerações e práticas recomendadas para a instalação e o cabeamento das gavetas de disco.

O *Installation and Service Guide* do modelo de compartimento de disco descreve as considerações e as práticas recomendadas.

- O computador que você está usando para configurar as bridges deve estar executando um navegador da Web compatível com ATTO para usar a GUI ATTO ExpressNAV.

As Notas de versão do produto *ATTO* têm uma lista atualizada de navegadores da Web compatíveis. Você pode acessar este documento a partir do SITE DA ATTO, conforme descrito nas etapas a seguir.

Passos

1. Faça o download do *Installation and Service Guide* do modelo do compartimento de disco:
 - a. Acesse o site DA ATTO usando o link fornecido para o modelo do FibreBridge e baixe o manual e o utilitário Quicknav.



O *ATTO FibreBridge Installation and Operation Manual* para sua ponte de modelo tem mais informações sobre interfaces de gerenciamento.

Você pode acessar este e outros conteúdos no SITE DA ATTO usando o link fornecido na página Descrição DO ATTO Fibrebridge.

2. Reúna o hardware e as informações necessárias para usar as interfaces de gerenciamento de bridge recomendadas, a GUI ATTO ExpressNAV e o utilitário ATTO Quicknav:
 - a. Determine um nome de usuário e uma senha não padrão (para acessar as pontes).

Você deve alterar o nome de usuário e a senha padrão.
 - b. Se estiver configurando para gerenciamento IP das pontes, você precisará do cabo Ethernet blindado fornecido com as pontes (que se 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 compartimentos de disco, controladores FC e dispositivos de fita de backup usando cabos de fibra ótica multimodo de 50 micrões, 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

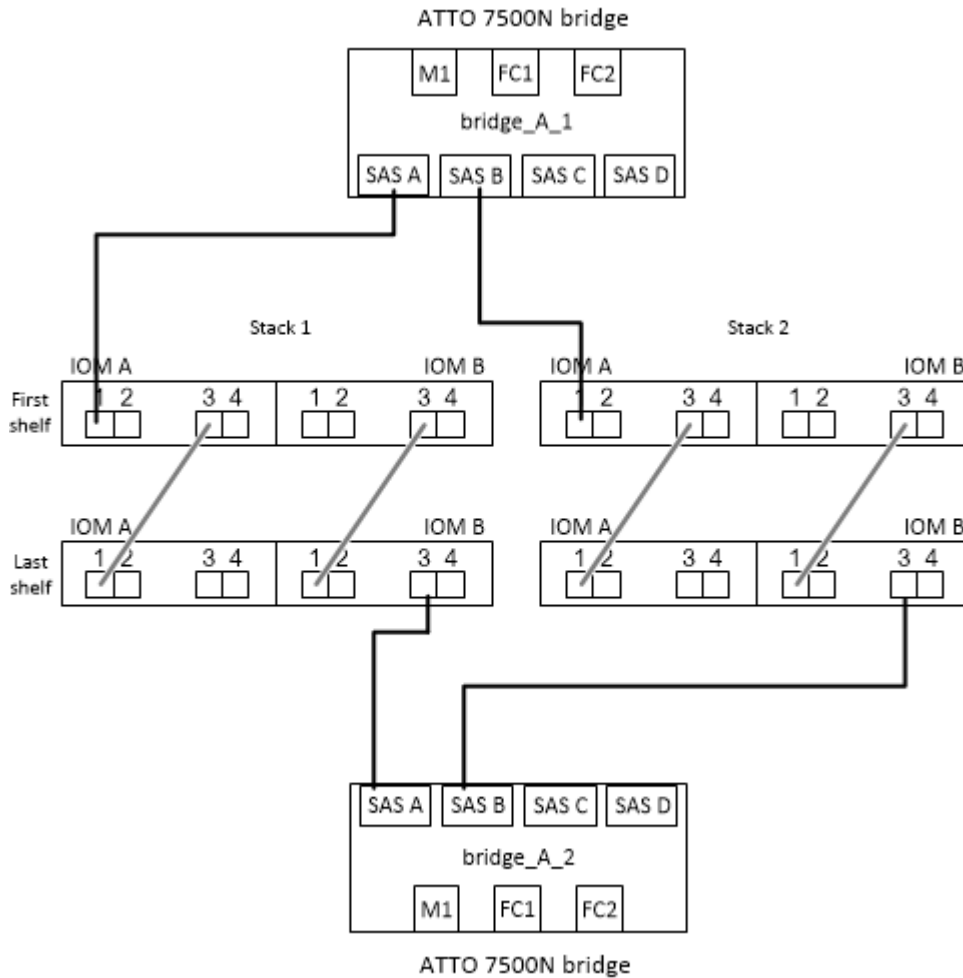
1. Encadeie em série as gavetas de disco em cada pilha:
 - a. Começando pela primeira gaveta lógica na stack, conecte IOM A porta 3 à IOM A porta 1 à IOM A na próxima gaveta até que cada IOM A na stack seja conectada.
 - b. Repita o subpasso anterior para IOM B.
 - c. Repita as subetapas anteriores para cada pilha.

O [Installation and Service Guide](#) do modelo de compartimento de disco fornece informações detalhadas sobre as prateleiras de disco em encadeamento em série.
2. Ligue as gavetas de disco e, em seguida, defina as IDs de gaveta.
 - É necessário desligar cada compartimento de disco.
 - As IDs de gaveta devem ser exclusivas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster (incluindo ambos os locais).
3. Cable disk shelves to the FibreBridge bridges.
 - a. Para a primeira stack de gavetas de disco, cable IOM A da primeira gaveta para a porta SAS a na FibreBridge A e cable IOM B da última gaveta para a porta SAS a na FibreBridge B.
 - b. Para stacks de gaveta adicionais, repita a etapa anterior usando a próxima porta SAS disponível nas bridges do FibreBridge, usando a porta B para a segunda stack, a porta C para a terceira stack e a porta D para a quarta stack.
 - c. Durante o cabeamento, 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

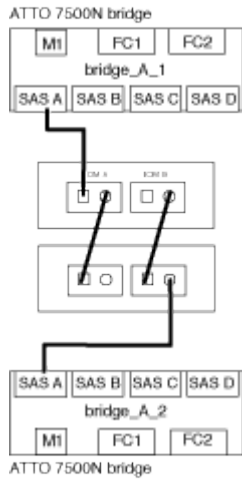
1. Encadeie as prateleiras em cada pilha.
 - a. Para a primeira stack de gavetas, cable IOM Uma porta quadrada da primeira gaveta para a porta SAS A na FibreBridge A.
 - b. Para a primeira stack de gavetas, a porta circular IOM B do cabo da última gaveta até a porta SAS A no FibreBridge B.

O *Installation and Service Guide* para o modelo de prateleira fornece informações detalhadas sobre

prateleiras de encadeamento em série.

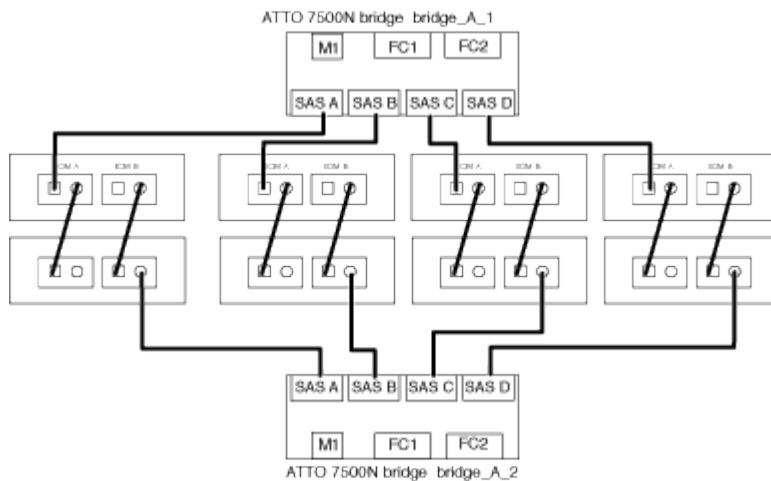
"Guia de instalação e serviço das gavetas de disco SAS para DS4243, DS2246, DS4486 e DS4246"

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 conectadas a um par de pontes FibreBridge 7600N ou 7500N.



Verifique a conectividade de ponte e faça o cabeamento das pontes FC para SAS às portas FC do controlador

É necessário fazer o cabeamento das pontes às portas FC do controlador em uma configuração MetroCluster conectada a ponte de dois nós.

Passos

1. Verifique se cada bridge pode detectar todas as unidades de disco e prateleiras de disco às quais a ponte está conectada:

```
sastargets
```

O `sastargets` comando output mostra os dispositivos (discos e prateleiras de discos) conectados à ponte. As linhas de saída são numeradas sequencialmente para que você possa contar rapidamente os

dispositivos.

A saída a seguir mostra que 10 discos estão 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

2. Verifique se o comando output mostra que a ponte está conectada aos discos e compartimentos de disco corretos na pilha.

Se a saída for...	Então...
Correto	Repita Passo 1 para cada ponte restante.
Não está correto	<ol style="list-style-type: none">Verifique se há cabos SAS soltos ou corrija o cabeamento SAS reabilitando as gavetas de disco nas pontes. Cable disk shelves to the bridgesRepita Passo 1 para cada ponte restante.

3. Cable cada bridge para as portas FC do controlador:

a. Cabo FC porta 1 da ponte para uma porta FC no controlador em cluster_A.

b. Cabo FC porta 2 da ponte para uma porta FC no controlador em cluster_B.

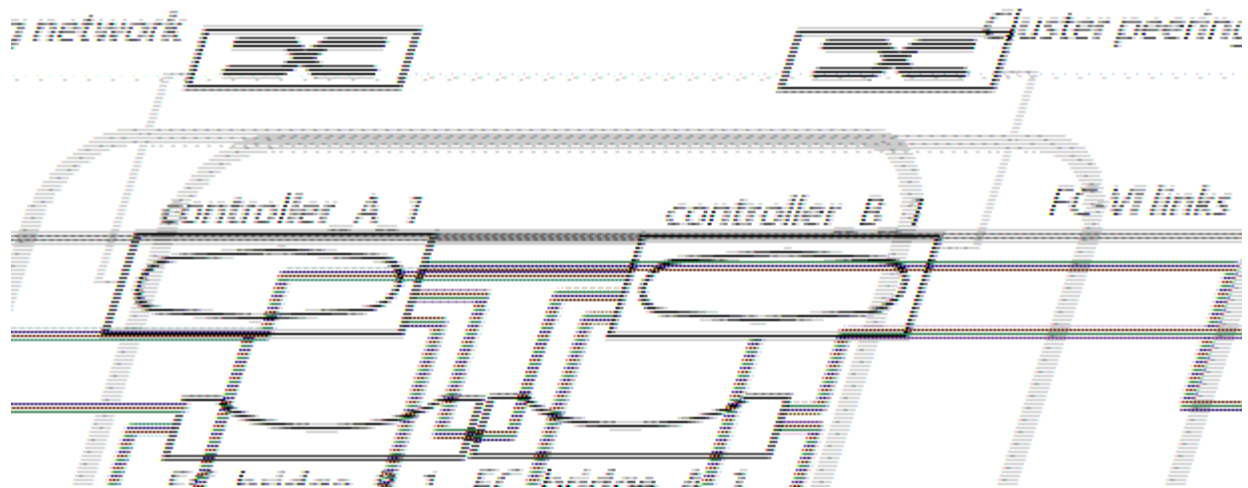
- Se o controlador estiver configurado com um adaptador FC de quatro portas, certifique-se de que as bridges em ambas as extremidades da pilha de armazenamento não estejam conectadas a duas portas FC no mesmo ASIC. Por exemplo:

- O porto a e o porto b compartilham o mesmo ASIC.
- A porta c e a porta d compartilham o mesmo ASIC.

Neste exemplo, conecte FC_bridge_A_1 à porta a e FC_bridge_A2 à porta c.

- Se o controlador estiver configurado com mais de um adaptador FC, não faça o cabeamento das pontes de ambas as extremidades da pilha de storage ao mesmo adaptador.

Nesse cenário, você deve conectar FC_bridge_A_1 a uma porta FC integrada e conectar FC_bridge_A_2 a uma porta FC em um adaptador em um slot de expansão.



4. Repita [Passo 3](#) nas outras pontes até que todas as pontes tenham sido cabeadas.

Proteja ou desproteja 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 desproteja a ponte.

- O seguinte comando protege `bridge_A_1`:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
```

- O comando a seguir desprotege `bridge_A_1`:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. No prompt ONTAP do cluster que contém a ponte, salve a configuração da ponte:

```
storage bridge run-cli -bridge <bridge-name> -command saveconfiguration
```

O seguinte comando protege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command  
saveconfiguration
```

3. No prompt ONTAP do cluster que contém a ponte, reinicie o firmware da ponte:

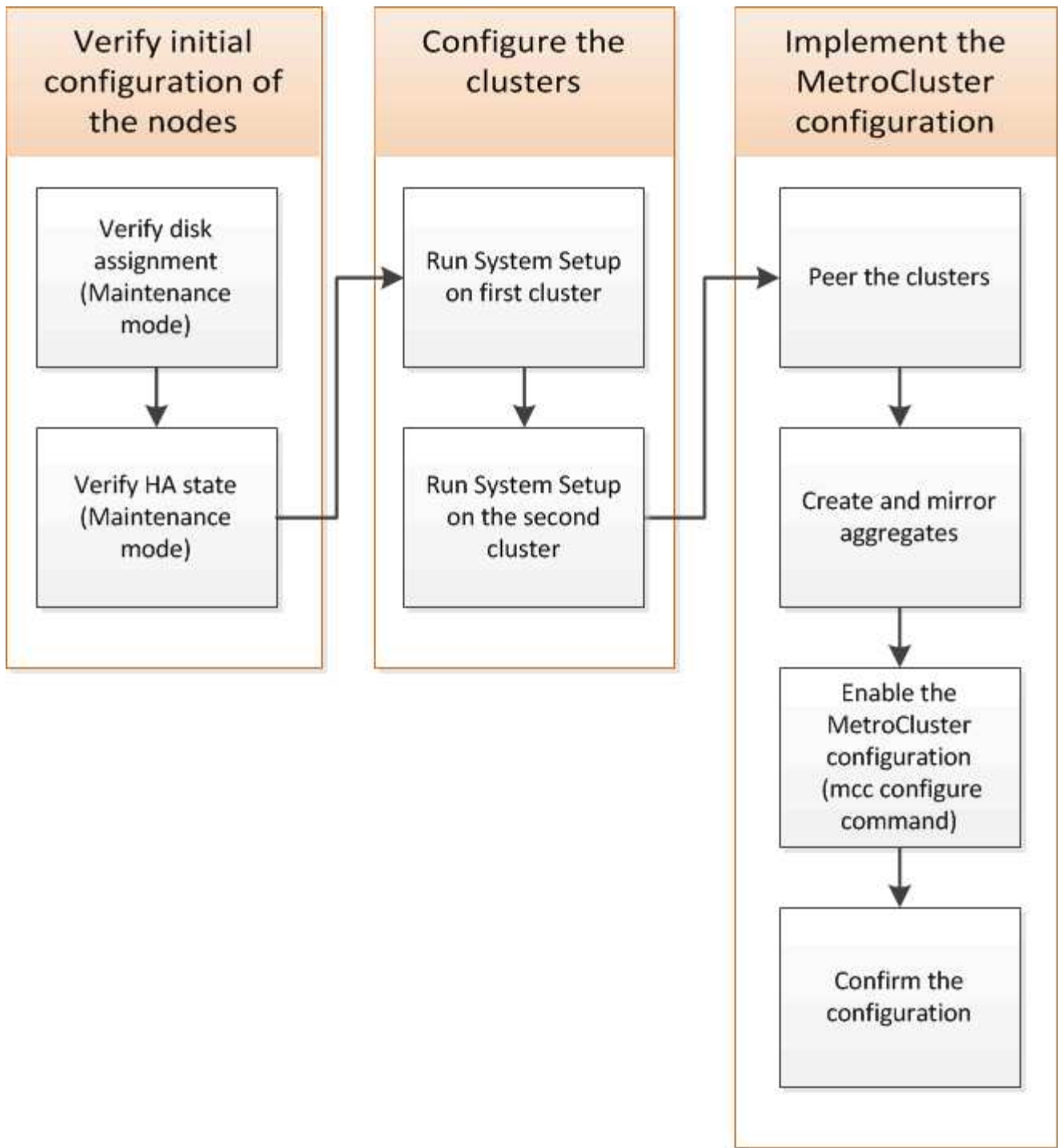
```
storage bridge run-cli -bridge <bridge-name> -command firmwarerestart
```

O seguinte comando protege bridge_A_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```

Configurando o software MetroCluster no ONTAP

É necessário configurar cada nó na configuração do MetroCluster no ONTAP, incluindo as configurações no nível do nó e a configuração dos nós em dois locais. Você também deve implementar a relação MetroCluster entre os dois sites.



Passos

1. Reúna os endereços IP necessários para os módulos do controlador antes de iniciar o processo de configuração.
2. Preencha a Planilha de informações de rede IP para o local A..

Folha de cálculo de informações de rede IP para o local A

Você deve obter endereços IP e outras informações de rede para o primeiro site do MetroCluster (site A) do administrador da rede antes de configurar o sistema.

Site Um cluster de criação de informações

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster. Exemplo usado nesta informação: Site_A	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do site A.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1. Exemplo usado nesta informação: Controller_A_1				
Nó 2. Não é necessário se estiver usando a configuração MetroCluster de dois nós (um nó em cada local). Exemplo usado nesta informação: Controller_A_2				

Crie um site LIFs e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				

Nó 1 IC LIF 2				
---------------	--	--	--	--

Site A informações do servidor de tempo

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local A Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		Anfitriões de correio
Endereços IP ou nomes		Protocolo de transporte
HTTP, HTTPS OU SMTP		Servidor proxy
	Endereços de e-mail do destinatário ou listas de distribuição	Mensagens completas
	Mensagens concisas	

Site A informações do SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção. Isso requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1			

Folha de cálculo de informações de rede IP para o local B.

Você deve obter endereços IP e outras informações de rede para o segundo site da MetroCluster (site B) do administrador da rede antes de configurar o sistema.

Informações sobre a criação do cluster do local B.

Quando você cria o cluster pela primeira vez, você precisa das seguintes informações:

Tipo de informação	Seus valores
Nome do cluster. Exemplo usado nesta informação: Site_B	
Domínio DNS	
Servidores de nomes DNS	
Localização	
Senha do administrador	

Informações do nó do local B.

Para cada nó no cluster, é necessário um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão.

Nó	Porta	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1. Exemplo usado nesta informação: Controller_B_1				
Nó 2. Não é necessário para configurações de MetroCluster de dois nós (um nó em cada local). Exemplo usado nesta informação: Controller_B_2				

LIFs do local B e portas para peering de cluster

Para cada nó no cluster, você precisa dos endereços IP de duas LIFs entre clusters, incluindo uma máscara de rede e um gateway padrão. Os LIFs entre clusters são usados para fazer o peer dos clusters.

Nó	Porta	Endereço IP do LIF entre clusters	Máscara de rede	Gateway predefinido
Nó 1 IC LIF 1				
Nó 1 IC LIF 2				

Informações do servidor de hora local B.

É necessário sincronizar a hora, que requer um ou mais servidores de hora NTP.

Nó	Nome do host	Endereço IP	Máscara de rede	Gateway predefinido
Servidor NTP 1				
Servidor NTP 2				

Local B Informação AutoSupport

Você deve configurar o AutoSupport em cada nó, o que requer as seguintes informações:

Tipo de informação		Seus valores
Do endereço de e-mail		Anfitriões de correio
Endereços IP ou nomes		Protocolo de transporte
HTTP, HTTPS OU SMTP		Servidor proxy
	Endereços de e-mail do destinatário ou listas de distribuição	Mensagens completas
	Mensagens concisas	

Local B Informação SP

Você deve habilitar o acesso ao processador de serviço (SP) de cada nó para solução de problemas e manutenção, o que requer as seguintes informações de rede para cada nó:

Nó	Endereço IP	Máscara de rede	Gateway predefinido
Nó 1 (controlador_B_1)			

Semelhanças e diferenças entre configurações padrão de cluster e MetroCluster

A configuração dos nós em cada cluster em uma configuração MetroCluster é semelhante à dos nós em um cluster padrão.

A configuração do MetroCluster é baseada em dois clusters padrão. Fisicamente, a configuração deve ser simétrica, com cada nó tendo a mesma configuração de hardware e todos os componentes do MetroCluster devem ser cabeados e configurados. No entanto, a configuração básica de software para nós em uma configuração MetroCluster é a mesma para nós em um cluster padrão.

Etapa de configuração	Configuração padrão de cluster	Configuração do MetroCluster
-----------------------	--------------------------------	------------------------------

Configurar LIFs de gerenciamento, cluster e dados em cada nó.	O mesmo em ambos os tipos de clusters	Configure o agregado raiz.
O mesmo em ambos os tipos de clusters	Configure o cluster em um nó no cluster.	O mesmo em ambos os tipos de clusters
Junte o outro nó ao cluster.	O mesmo em ambos os tipos de clusters	Crie um agregado de raiz espelhado.
Opcional	Obrigatório	Espreite os clusters.
Opcional	Obrigatório	Ative a configuração do MetroCluster.

Restaurando os padrões do sistema e configurando o tipo HBA em um módulo do controlador

Para garantir uma instalação bem-sucedida do MetroCluster, redefina e restaure padrões nos módulos do controlador.

Importante

Essa tarefa só é necessária para configurações Stretch usando bridges FC-para-SAS.

Passos

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

```
set-defaults
```

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

- a. Arranque no modo de manutenção:

```
boot_ontap maint
```

- b. Verifique as definições atuais das portas:

```
ucadmin show
```

- c. Atualize as definições da porta conforme necessário.

Se você tem este tipo de HBA e modo desejado...	Use este comando...
CNA FC	<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 dois nós

Antes de iniciar totalmente o sistema no ONTAP, você pode opcionalmente inicializar o sistema no modo Manutenção e verificar a atribuição de disco nos nós. Os discos devem ser atribuídos para criar uma configuração totalmente simétrica, com os dois locais que possuem suas próprias gavetas de disco e fornecimento de dados, em que cada nó e cada pool têm um número igual de discos espelhados atribuídos a eles.

Antes de começar

O sistema tem de estar no modo de manutenção.

Sobre esta tarefa

Os novos sistemas MetroCluster têm atribuições de disco concluídas antes do envio.

A tabela a seguir mostra exemplos de atribuições de pool para uma configuração do MetroCluster. Os discos são atribuídos a pools por compartimento.

Compartimento de disco (exemplo nome)...	No local...	Pertence a...	E é atribuído a esse nó...
Compartimento de disco 1 (shelf_A_1_1)	Local A	Nó A 1	Piscina 0
Compartimento de disco 2 (shelf_A_1_3)	Compartimento de disco 3 (gaveta_B_1_1)	Nó B 1	Piscina 1
Compartimento de disco 4 (gaveta_B_1_3)	Compartimento de disco 9 (gaveta_B_1_2)	Local B	Nó B 1
Piscina 0	Compartimento de disco 10 (gaveta_B_1_4)	Compartimento de disco 11 (shelf_A_1_2)	Nó A 1

Se a configuração incluir DS460C compartimentos de disco, você deve atribuir manualmente os discos usando as seguintes diretrizes para cada gaveta de 12 discos:

Atribuir estes discos na gaveta...	Para este nó e pool...
1 - 6	Pool do nó local 0
7 - 12	Pool do parceiro DR 1

Esse padrão de atribuição de disco minimiza o efeito em um agregado se uma gaveta ficar offline.

Passos

1. Se o seu sistema foi recebido de fábrica, confirme as atribuições de prateleira:

```
disk show -v
```

2. Se necessário, você pode atribuir explicitamente discos nas gavetas de disco conectadas ao pool apropriado

```
disk assign
```

Os compartimentos de disco no mesmo local que o nó são atribuídos ao pool 0 e os compartimentos de disco localizados no local do parceiro são atribuídos ao pool 1. Você deve atribuir um número igual de prateleiras a cada pool.

- a. Se você não tiver feito isso, inicialize cada sistema no modo Manutenção.
- b. No nó no local A, atribua sistematicamente as gavetas de disco locais ao pool 0 e às gavetas de disco remotas ao pool 1: Mais `disk assign -shelf disk_shelf_name -p pool`

Se o nó_A_1 do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

- c. No nó do local remoto (local B), atribua sistematicamente suas gavetas de disco locais ao pool 0 e suas gavetas de disco remotas ao pool 1: Mais `disk assign -shelf disk_shelf_name -p pool`

Se o nó `B_1` do controlador de storage tiver quatro compartimentos, você emitirá os seguintes comandos:

```
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
```

- a. Mostrar as IDs e os compartimentos do compartimento de disco para cada disco `disk show -v`

Verificando o estado de HA dos componentes

Em uma configuração Stretch MetroCluster que não está pré-configurada na fábrica, você deve verificar se o estado HA do controlador e do componente do chassi está definido como "mcc-2n" para que eles iniciem corretamente. Para sistemas recebidos de fábrica, esse valor é pré-configurado e você não precisa verificá-lo.

Antes de começar

O sistema tem de estar no modo de manutenção.

Passos

1. No modo de manutenção, visualize o estado HA do módulo do controlador e do chassis:

```
ha-config show
```

O módulo do controlador e o chassi devem mostrar o valor "mcc-2n".

2. Se o estado do sistema exibido do controlador não for "mcc-2n", defina o estado HA para o controlador:

```
ha-config modify controller mcc-2n
```

3. Se o estado do sistema exibido do chassi não for "mcc-2n", defina o estado HA para o chassi:

```
ha-config modify chassis mcc-2n
```

Parar o nó.

Aguarde até que o nó volte ao prompt DO Loader.

4. Repita estas etapas em cada nó na configuração do MetroCluster.

Configurando o ONTAP em uma configuração de MetroCluster de dois nós

Em uma configuração de MetroCluster de dois nós, em cada cluster, você deve inicializar o nó, sair do assistente de configuração de cluster e usar o `cluster setup` comando para configurar o nó em um cluster de nó único.

Antes de começar

Você não deve ter configurado o processador de serviço.

Sobre esta tarefa

Essa tarefa é para configurações de MetroCluster de dois nós que usam storage nativo do NetApp.

Essa tarefa deve ser executada em ambos os clusters na configuração do MetroCluster.

Para obter mais informações gerais sobre a configuração do ONTAP, consulte a. ["Configuração do ONTAP"](#)

Passos

1. Ligue o primeiro nó.



Repita esta etapa no nó no local de recuperação de desastres (DR).

O nó é inicializado e, em seguida, o assistente de Configuração de cluster é iniciado no console informando que o AutoSupport será ativado automaticamente.

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

You can enter the following commands at any time:

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.
```

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
<http://support.netapp.com/autosupport/>

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

```
Enter the node management interface port [e0M]:
```

```
Enter the node management interface IP address [10.101.01.01]:
```

```
Enter the node management interface netmask [101.010.101.0]:
```

```
Enter the node management interface default gateway [10.101.01.0]:
```

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

2. Criar um novo cluster:

```
create
```

3. Escolha se o nó deve ser usado como um cluster de nó único.

```
Do you intend for this node to be used as a single node cluster? {yes,  
no} [yes]:
```

4. Aceite o padrão do sistema "sim" pressionando Enter, ou insira seus próprios valores digitando "não" e,

em seguida, pressionando Enter.

5. Siga as instruções para concluir o assistente **Configuração de cluster**, pressione Enter para aceitar os valores padrão ou digitar seus próprios valores e pressione Enter.

Os valores padrão são determinados automaticamente com base na sua plataforma e configuração de rede.

6. Depois de concluir o assistente **Cluster Setup** e ele sair, verifique se o cluster está ativo e se o primeiro nó está em bom estado:

```
cluster show
```

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

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

Se for necessário alterar qualquer uma das configurações inseridas para o SVM admin ou nó SVM, você poderá acessar o assistente **Configuração de cluster** usando o `cluster setup` comando.

Configuração dos clusters em uma configuração do MetroCluster

É necessário fazer peer nos clusters, espelhar os agregados raiz, criar um agregado de dados espelhados e, em seguida, emitir o comando para implementar as operações do MetroCluster.

Peering dos clusters

Os clusters na configuração do MetroCluster precisam estar em um relacionamento de mesmo nível para que possam se comunicar uns com os outros e executar o espelhamento de dados essencial para a recuperação de desastres do MetroCluster.

Informações relacionadas

["Configuração expressa de peering de cluster e SVM"](#)

["Considerações ao usar portas dedicadas"](#)

["Considerações ao compartilhar portas de dados"](#)

Configurando LIFs entre clusters

É necessário criar LIFs entre clusters nas portas usadas para comunicação entre os clusters de parceiros da MetroCluster. Você pode usar portas dedicadas ou portas que também têm tráfego de dados.

Configurando LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra as portas de rede em "cluster01":

```
cluster01::> network port show
```

							Speed
(Mbps)							
Node	Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----	
cluster01-01							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
	e0e	Default	Default		up	1500	auto/1000
	e0f	Default	Default		up	1500	auto/1000
cluster01-02							
	e0a	Cluster	Cluster		up	1500	auto/1000
	e0b	Cluster	Cluster		up	1500	auto/1000
	e0c	Default	Default		up	1500	auto/1000
	e0d	Default	Default		up	1500	auto/1000
	e0e	Default	Default		up	1500	auto/1000
	e0f	Default	Default		up	1500	auto/1000

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

```
network interface show -fields home-port,curr-port
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os portos "e0e" e "e0f" não foram atribuídos LIFs:

```

cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port

Cluster cluster01-01_clus1  e0a        e0a
Cluster cluster01-01_clus2  e0b        e0b
Cluster cluster01-02_clus1  e0a        e0a
Cluster cluster01-02_clus2  e0b        e0b
cluster01
    cluster_mgmt            e0c        e0c
cluster01
    cluster01-01_mgmt1      e0c        e0c
cluster01
    cluster01-02_mgmt1      e0c        e0c

```

3. Crie um grupo de failover para as portas dedicadas:

```

network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical_or_logical_ports

```

O exemplo a seguir atribui as portas "e0e" e "e0f" ao grupo de failover "intercluster01" no SVM do sistema "cluster01":

```

cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f

```

4. Verifique se o grupo de failover foi criado:

```

network interface failover-groups show

```

Para obter a sintaxe completa do comando, consulte a página [man](#).

```

cluster01::> network interface failover-groups show

```

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.

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<pre> 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 </pre>
ONTAP 9 F.5 e anteriores	<pre> 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 </pre>

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" no grupo de failover "intercluster01":


```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. Verifique se as LIFs entre clusters foram criadas:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9 F.5 e anteriores	<code>network interface show -role intercluster</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

```

cluster01::> network interface show -service-policy default-intercluster
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
-----
cluster01
      cluster01_icl01
              up/up      192.168.1.201/24  cluster01-01  e0e
true
      cluster01_icl02
              up/up      192.168.1.202/24  cluster01-02  e0f
true

```

7. Verifique se as LIFs entre clusters são redundantes:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<code>network interface show -service-policy default-intercluster -failover</code>

Em ONTAP 9.5 e anteriores

```
network interface show -role intercluster -failover
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta SVM "e0e" falharão para a porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface          Node:Port          Policy            Group
-----  -
cluster01
          cluster01_icl01 cluster01-01:e0e  local-only
intercluster01
                                Failover Targets: cluster01-01:e0e,
                                                cluster01-01:e0f
          cluster01_icl02 cluster01-02:e0e  local-only
intercluster01
                                Failover Targets: cluster01-02:e0e,
                                                cluster01-02:e0f
```

Informações relacionadas

["Considerações ao usar portas dedicadas"](#)

Configurando LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra as portas de rede em "cluster01":

```

cluster01::> network port show

(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU   Admin/Oper
-----
cluster01-01
  e0a    Cluster   Cluster      up    1500  auto/1000
  e0b    Cluster   Cluster      up    1500  auto/1000
  e0c    Default   Default      up    1500  auto/1000
  e0d    Default   Default      up    1500  auto/1000
cluster01-02
  e0a    Cluster   Cluster      up    1500  auto/1000
  e0b    Cluster   Cluster      up    1500  auto/1000
  e0c    Default   Default      up    1500  auto/1000
  e0d    Default   Default      up    1500  auto/1000

```

2. Criar LIFs entre clusters no sistema:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service-policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
ONTAP 9 F.5 e anteriores	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir cria LIFs entre clusters "cluster01_icl01" e "cluster01_icl02":

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

3. Verifique se as LIFs entre clusters foram criadas:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<code>network interface show -service-policy default-intercluster</code>
ONTAP 9 F.5 e anteriores	<code>network interface show -role intercluster</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

```
cluster01::> network interface show -service-policy default-intercluster
      Logical      Status      Network      Current
Current Is
Vserver  Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
cluster01
      cluster01_icl01
              up/up      192.168.1.201/24  cluster01-01  e0c
true
      cluster01_icl02
              up/up      192.168.1.202/24  cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

Versão de ONTAP	Comando
ONTAP 9 F.6 e mais tarde	<code>network interface show -service-policy default-intercluster -failover</code>
ONTAP 9 F.5 e anteriores	<code>network interface show -role intercluster -failover</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra que os LIFs entre clusters "cluster01_icl01" e "cluster01_icl02" na porta "e0c" falharão para a porta "e0d".

```

cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface          Node:Port          Policy          Group
-----  -
cluster01
          cluster01_icl01 cluster01-01:e0c  local-only
192.168.1.201/24
                                Failover Targets: cluster01-01:e0c,
                                                cluster01-01:e0d
          cluster01_icl02 cluster01-02:e0c  local-only
192.168.1.201/24
                                Failover Targets: cluster01-02:e0c,
                                                cluster01-02:e0d

```

Informações relacionadas

["Considerações ao compartilhar portas de dados"](#)

Criando um relacionamento de cluster peer

É necessário criar o relacionamento de peers de clusters entre os clusters do MetroCluster.

Criando um relacionamento de cluster peer

Você pode usar o `cluster peer create` comando para criar uma relação entre pares entre um cluster local e remoto. Após a criação da relação de pares, você pode executar `cluster peer create` no cluster remoto para autenticá-la no cluster local.

Antes de começar

- Você precisa ter criado LIFs entre clusters em todos os nós nos clusters que estão sendo perados.
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior.

Passos

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

```

cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY
HH:MM:SS|1...7days|1...168hours -peer-addr peer_LIF_IPs -ip-space ip-space

```

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 `-ip-space` 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 -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 nos endereços IP 192.140.112.101 e 192.140.112.102 do LIF:

```
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 -ip-space ip-space
```

Você pode ignorar a `-ip-space` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria uma relação de peer de cluster com o cluster remoto nos endereços IP de LIF 192.168.2.201 e 192.168.2.202:

```
cluster02::> cluster peer create -peer-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 nos endereços IP 192.140.112.203 e 192.140.112.204 do LIF:

```
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"](#)

["Conceitos de ONTAP"](#)

Criando um agregado de dados espelhados em cada nó

Você precisa criar um agregado de dados espelhados em cada nó no grupo de DR.

Antes de começar

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode garantir que o tipo de unidade correto esteja selecionado.

Sobre esta tarefa

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.

["Gerenciamento de disco e agregado"](#)

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

```
storage disk show -spare -owner node_name
```

2. Criar o agregado:

```
storage aggregate create -mirror true
```

Se você estiver 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 mínima suportada, na qual um número limitado de unidades está disponível, você deve usar a opção `force-small-Aggregate` para permitir a criação de um agregado RAID-DP de três discos.

- Estilo de checksum para usar para o agregado
- Tipo de unidades a utilizar
- Tamanho das unidades a utilizar
- Velocidade de condução a utilizar
- Tipo RAID para grupos RAID no agregado
- Número máximo de unidades ou LUNs de storage que podem ser incluídos em um grupo RAID
- Se unidades com RPM diferentes são permitidas para obter mais informações sobre essas opções, consulte a `storage aggregate create` página de manual.

O comando a seguir cria um agregado espelhado com 10 discos:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

```
storage aggregate show-status -aggregate aggregate-name
```

Criação de agregados de dados sem espelhamento

Você pode, opcionalmente, criar agregados de dados sem espelhamento para dados que não exigem o espelhamento redundante fornecido pelas configurações do MetroCluster.

Antes de começar

- Você deve saber quais unidades ou LUNs de array serão usados no novo agregado.
- Se você tiver vários tipos de unidade no sistema (armazenamento heterogêneo), você deve entender como pode verificar se o tipo de unidade correto está selecionado.

Exemplo 1. Sobre esta tarefa

ATENÇÃO: Nas configurações MetroCluster FC, os agregados sem espelhamento só estarão online após um switchover se os discos remotos no agregado estiverem acessíveis. Se os ISLs falharem, o nó local poderá não conseguir aceder aos dados nos discos remotos sem espelhamento. A falha de um agregado pode levar a uma reinicialização do nó local.



Os agregados sem espelhamento devem ser locais para o nó que os possui.

- As unidades e LUNs de array são de propriedade de um nó específico. Quando você cria um agregado, todas as unidades nesse agregado precisam ser de propriedade do mesmo nó, que se torna o nó inicial desse agregado.
- Os nomes agregados devem estar em conformidade com o esquema de nomenclatura que você determinou quando você planejou sua configuração do MetroCluster.
- O "[Gerenciamento de discos e agregados](#)" contém mais informações sobre o espelhamento de agregados.

Passos

1. Apresentar uma lista de peças sobresselentes disponíveis:

```
storage disk show -spare -owner node_name
```

2. Criar o agregado:

```
storage aggregate create
```

Se você estiver 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 `storage aggregate create` página de manual.

O comando a seguir cria um agregado sem espelhamento com 10 discos:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verifique o grupo RAID e as unidades do seu novo agregado:

```
storage aggregate show-status -aggregate aggregate-name
```

Implementando a configuração do MetroCluster

Você deve executar o `metrocluster configure` comando para iniciar a proteção de dados em uma configuração do MetroCluster.

Antes de começar

- Deve haver pelo menos dois agregados de dados espelhados não-raiz em cada cluster.

Agregados de dados adicionais podem ser espelhados ou sem espelhamento.

Verifique os tipos de agregados:

```
storage aggregate show
```



Se você quiser usar um único agregado de dados espelhados, consulte ["Configurar o software MCC no ONTAP"](#) para obter instruções.

- O estado ha-config dos controladores e chassis deve ser "mcc-2n".

Sobre esta tarefa

Você pode emitir o `metrocluster configure` comando uma vez, em qualquer um dos nós, para ativar a configuração do MetroCluster. Você não precisa emitir o comando em cada um dos sites ou nós, e não importa em qual nó ou site você escolher emitir o comando.

Passos

1. Configure o MetroCluster no seguinte formato:

Se a sua configuração do MetroCluster tiver...	Então faça isso...
Vários agregados de dados	A partir do prompt de qualquer nó, configure o MetroCluster: <pre>metrocluster configure node-name</pre>

Um único agregado de dados espelhados

a. A partir do prompt de qualquer nó, altere para o nível de privilégio avançado:

```
set -privilege advanced
```

Você precisa responder com "y" quando for solicitado a continuar para o modo avançado e você vir o prompt do modo avançado (*>).

b. Configure o MetroCluster com o `-allow-with-one-aggregate true` parâmetro:

```
metrocluster configure -allow-with-one-aggregate true node-name
```

c. Voltar para o nível de privilégio de administrador `set -privilege admin`



A prática recomendada é ter vários agregados de dados. Se o primeiro grupo de DR tiver apenas um agregado e quiser adicionar um grupo de DR com um agregado, mova o volume de metadados do agregado de dados único. Para obter mais informações sobre este procedimento, "[Movimentação de um volume de metadados nas configurações do MetroCluster](#)" consulte .

O comando a seguir habilita a configuração do MetroCluster em todos os nós do grupo DR que contém "controller_A_1":

```
cluster_A::*> metrocluster configure -node-name controller_A_1  
  
[Job 121] Job succeeded: Configure is successful.
```

2. Verifique o status da rede no local A:

```
network port show
```

O exemplo a seguir mostra o uso da porta de rede:

```
cluster_A::> network port show
```

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

```
7 entries were displayed.
```

3. Verifique a configuração do MetroCluster de ambos os sites na configuração do MetroCluster.

a. Verifique a configuração a partir do site A `metrocluster show`

```
cluster_A::> metrocluster show
```

Cluster	Entry Name	State

Local: cluster_A	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
	disaster	
Remote: cluster_B	Configuration state	configured
	Mode	normal
	AUSO Failure Domain	auso-on-cluster-
	disaster	

b. Verifique a configuração a partir do local B `metrocluster show`

```

cluster_B::> metrocluster show
Cluster                Entry Name                State
-----
Local: cluster_B      Configuration state        configured
                        Mode                        normal
                        AUSO Failure Domain        auso-on-cluster-
disaster
Remote: cluster_A     Configuration state        configured
                        Mode                        normal
                        AUSO Failure Domain        auso-on-cluster-
disaster

```

Configuração de pontes FC para SAS para monitoramento de integridade

Em sistemas que executam versões do ONTAP anteriores a 9,8, se sua configuração incluir pontes FC para SAS, você deverá executar algumas etapas especiais de configuração para monitorar as pontes FC para SAS na configuração do MetroCluster.

- Ferramentas de monitoramento SNMP de terceiros não são suportadas para bridges FibreBridge.
- A partir do ONTAP 9.8, as bridges FC para SAS são monitoradas por meio de conexões na banda por padrão, e não é necessária configuração adicional.



A partir de ONTAP 9.8, o `storage bridge` comando é substituído por `system bridge`. As etapas a seguir mostram o `storage bridge` comando, mas se você estiver executando o ONTAP 9.8 ou posterior, o `system bridge` comando é preferido.

Passos

1. No prompt do cluster do ONTAP, adicione a ponte ao monitoramento de integridade:
 - a. Adicione a ponte, usando o comando para sua versão do ONTAP:

Versão de ONTAP	Comando
ONTAP 9 F.5 e mais tarde	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>
ONTAP 9.4 e anteriores	<code>storage bridge add -address <i>bridge-ip-address</i> -name <i>bridge-name</i></code>

- b. Verifique se a ponte foi adicionada e está configurada corretamente:

```
storage bridge show
```

Pode levar até 15 minutos para refletir todos os dados por causa do intervalo de votação. O monitor de saúde do ONTAP pode entrar em Contato e monitorar a ponte se o valor na coluna "Status" for "ok", e outras informações, como o nome mundial (WWN), forem exibidas.

O exemplo a seguir mostra que as bridges FC para SAS estão configuradas:

```
controller_A_1::> storage bridge show

Bridge          Symbolic Name Is Monitored  Monitor Status  Vendor
Model          Bridge WWN
-----
-----
ATTO_10.10.20.10  atto01         true          ok              Atto
FibreBridge 7500N  20000010867038c0
ATTO_10.10.20.11  atto02         true          ok              Atto
FibreBridge 7500N  20000010867033c0
ATTO_10.10.20.12  atto03         true          ok              Atto
FibreBridge 7500N  20000010867030c0
ATTO_10.10.20.13  atto04         true          ok              Atto
FibreBridge 7500N  2000001086703b80

4 entries were displayed

controller_A_1::>
```

Verificar a configuração do MetroCluster

Você pode verificar se os componentes e as relações na configuração do MetroCluster estão funcionando corretamente. Você deve fazer uma verificação após a configuração inicial e depois de fazer quaisquer alterações na configuração do MetroCluster. Você também deve fazer uma verificação antes de um switchover negociado (planejado) ou de uma operação de switchback.

Se o `metrocluster check run` comando for emitido duas vezes dentro de um curto espaço de tempo em um ou em ambos os clusters, um conflito pode ocorrer e o comando pode não coletar todos os dados. Os comandos subsequentes `metrocluster check show` não mostram a saída esperada.

1. Verificar a configuração:

```
metrocluster check run
```

O comando é executado como um trabalho em segundo plano e pode não ser concluído imediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	ok
volumes	ok

7 entries were displayed.

2. Apresentar resultados mais detalhados:

```
metrocluster check run
```

```
metrocluster check aggregate show
```

```
metrocluster check cluster show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

Os `metrocluster check show` comandos mostram os resultados do comando mais recente `metrocluster check run`. Você deve sempre executar o `metrocluster check run` comando antes de usar os `metrocluster check show` comandos para que as informações exibidas sejam atuais.

O exemplo a seguir mostra a `metrocluster check aggregate show` saída do comando para uma configuração de MetroCluster de quatro nós saudável:

```
cluster_A::> metrocluster check aggregate show
```

```
Last Checked On: 8/5/2014 00:42:58
```

Node	Aggregate	Check
Result		
-----	-----	-----
controller_A_1	controller_A_1_aggr0	mirroring-status
ok		disk-pool-allocation

```

ok
ownership-state
ok
controller_A_1_aggr1
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_1_aggr2
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2
controller_A_2_aggr0
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2_aggr1
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
controller_A_2_aggr2
mirroring-status
ok
disk-pool-allocation
ok
ownership-state
ok
18 entries were displayed.

```

O exemplo a seguir mostra a `metrocluster check cluster show` saída do comando para uma configuração de MetroCluster de quatro nós saudável. Isso indica que os clusters estão prontos para executar um switchover negociado, se necessário.

Last Checked On: 9/13/2017 20:47:04

Cluster	Check	Result
mccint-fas9000-0102	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok
mccint-fas9000-0304	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok

10 entries were displayed.

Informações relacionadas

["Gerenciamento de disco e agregado"](#)

["Gerenciamento de rede e LIF"](#)

Verificando erros de configuração do MetroCluster com o Config Advisor

Você pode acessar o site de suporte da NetApp e baixar a ferramenta Config Advisor para verificar se há erros de configuração comuns.

O Config Advisor é uma ferramenta de validação de configuração e verificação de integridade. Você pode implantá-lo em sites seguros e sites não seguros para coleta de dados e análise do sistema.



O suporte para Config Advisor é limitado e está disponível apenas online.

1. Vá para a página de download do Config Advisor e baixe a ferramenta.

["NetApp Downloads: Config Advisor"](#)

2. Execute o Config Advisor, revise a saída da ferramenta e siga as recomendações na saída para resolver quaisquer problemas descobertos.

Verificando switchover, cura e switchback

Você deve verificar as operações de switchover, recuperação e switchback da configuração do MetroCluster.

1. Use os procedimentos para comutação negociada, cura e switchback que são mencionados no ["Execute switchover, cura e switchback"](#).

Protegendo arquivos de backup de configuração

Você pode fornecer proteção adicional para os arquivos de backup de configuração de cluster especificando um URL remoto (HTTP ou FTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster local.

1. Defina o URL do destino remoto para os arquivos de backup de configuração:

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

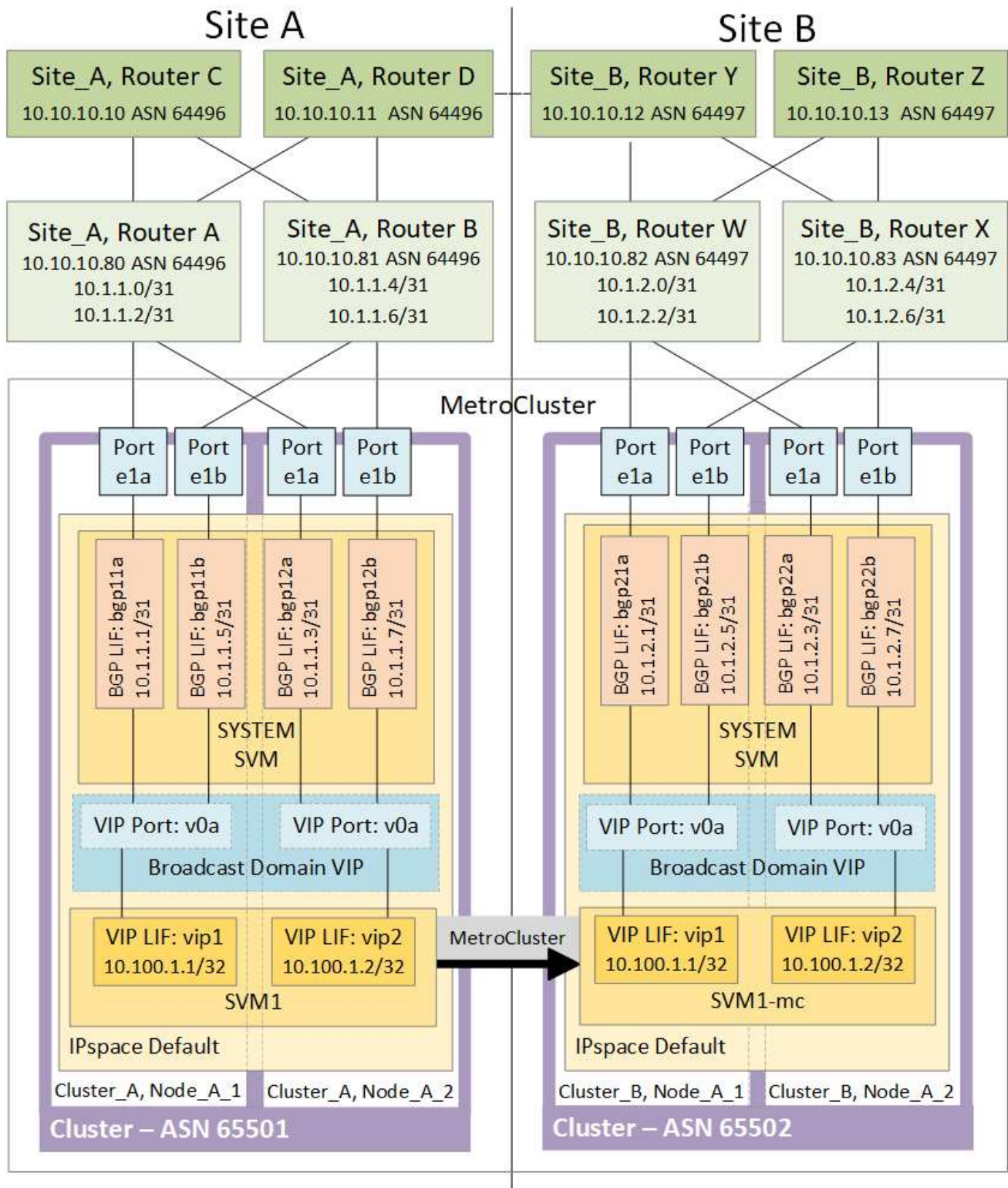
O ["Gerenciamento de clusters com a CLI"](#) contém informações adicionais na seção *Gerenciando backups de configuração*.

Considerações para usar IP virtual e protocolo de gateway de borda com uma configuração MetroCluster

A partir do ONTAP 9.5, o ONTAP oferece suporte à 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, consulte a seguinte seção:

["Configurando LIFs de IP virtual \(VIP\)"](#)



Limitações do ONTAP

O ONTAP não verifica automaticamente se todos os nós em ambos os sites da configuração do MetroCluster estão configurados com peering BGP.

O ONTAP não executa agregação de rotas, mas anuncia todos os IPs de LIF virtuais individuais como rotas

de host exclusivas em todos os momentos.

O ONTAP não suporta True anycast — apenas um único nó no cluster apresenta um IP de LIF virtual específico (mas é aceito por todas as interfaces físicas, independentemente de serem LIFs BGP, desde que a porta física faça parte do espaço IPspace correto). Diferentes LIFs podem migrar independentemente um do outro para diferentes nós de hospedagem.

Diretrizes para usar esta solução de camada 3 com uma configuração MetroCluster

Você deve configurar seu BGP e VIP corretamente para fornecer a redundância necessária.

Cenários de implantação mais simples são preferidos em relação a arquiteturas mais complexas (por exemplo, um roteador de peering BGP é acessível em um roteador intermediário não BGP). No entanto, o ONTAP não aplica restrições de design ou topologia de rede.

Os LIFs VIP cobrem apenas a rede frontend/data.

Dependendo da sua versão do ONTAP, você deve configurar LIFs de peering BGP no nó SVM, não no sistema ou na SVM de dados. No ONTAP 9.8, as LIFs de BGP são visíveis no SVM do cluster (sistema) e as SVMs de nó não estão mais presentes.

Cada SVM de dados requer a configuração de todos os endereços potenciais de gateway de primeiro salto (normalmente, o endereço IP de peering do roteador BGP), de modo que o caminho de dados de retorno esteja disponível se ocorrer uma migração de LIF ou failover de MetroCluster.

As LIFs BGP são específicas de nós, semelhantes às LIFs entre clusters - cada nó tem uma configuração exclusiva, que não precisa ser replicado para os nós do local de DR.

A existência do v0a (v0b e assim por diante) valida continuamente a 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 refletores de rota não são impossíveis, mas fora do escopo de uma configuração VIP direta.

Após a implantação, você deve verificar se o SVM de dados está acessível quando o LIF virtual associado é migrado entre todos os nós em cada local (incluindo switchover de MetroCluster) para verificar a configuração correta das rotas estáticas para o mesmo SVM de dados.

O VIP funciona para a maioria dos protocolos baseados em IP (NFS, SMB, iSCSI).

Testando a configuração do MetroCluster

Você pode testar cenários de falha para confirmar o funcionamento correto da configuração do MetroCluster.

Verificando o switchover negociado

Você pode testar uma operação de switchover negociado (planejada) para confirmar a disponibilidade de dados ininterrupta.

Este teste valida que a disponibilidade de dados não é afetada (exceto para os protocolos SMB (Server Message Block) da Microsoft e Fibre Channel do Solaris), alternando o cluster para o segundo data center.

Este teste deve levar cerca de 30 minutos.

Este procedimento tem os seguintes resultados esperados:

- O `metrocluster switchover` comando apresentará um prompt de aviso.

Se você responder **yes** ao prompt, o site do qual o comando é emitido mudará para o site do parceiro.

Para configurações IP do MetroCluster:

- Para o ONTAP 9.4 e versões anteriores:
 - Os agregados espelhados ficarão degradados após o switchover negociado.
- Para o ONTAP 9.5 e posterior:
 - Agregados espelhados permanecerão no estado normal se o storage remoto estiver acessível.
 - Os agregados espelhados ficarão degradados após o switchover negociado se o acesso ao storage remoto for perdido.
- Para o ONTAP 9.8 e posterior:
 - Agregados não espelhados localizados no local de desastre ficarão indisponíveis se o acesso ao storage remoto for perdido. Isso pode levar a uma interrupção do controlador.

Passos

1. Confirme se todos os nós estão no estado configurado e no modo normal:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show

Cluster                               Configuration State  Mode
-----                               -
Local: cluster_A                       configured           normal
Remote: cluster_B                       configured           normal
```

2. Inicie a operação de comutação:


```
metrocluster switchover
```

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Confirme se o cluster local está no estado configurado e no modo de comutação:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show

Cluster                               Configuration State      Mode
-----                               -
-----
Local: cluster_A                       configured                switchover
Remote: cluster_B                       not-reachable            -
      configured                    normal
```

4. Confirme se a operação de comutação foi bem-sucedida:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
    State: successful
  Start Time: 2/6/2016 13:28:50
    End Time: 2/6/2016 13:29:41
    Errors: -
```

5. Use os `vserver show` comandos e `network interface show` para verificar se as SVMs e LIFs de DR estão online.

Verificando a cura e a troca manual

Você pode testar as operações de reparo e `switchback manual` para verificar se a disponibilidade de dados não é afetada (exceto para configurações SMB e Solaris FC), alternando o cluster para o data center original após um `switchover` negociado.

Este teste deve levar cerca de 30 minutos.

O resultado esperado deste procedimento é que os serviços devem ser reenviados para os seus nós domésticos.

Passos

1. Verifique se a cicatrização está concluída:

```
metrocluster node show
```

O exemplo a seguir mostra a conclusão bem-sucedida do comando:

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      node_A_1      configured    enabled    heal roots
completed
      cluster_B
      node_B_2      unreachable  -          switched over
42 entries were displayed.metrocluster operation show
```

2. Verifique se todos os agregados são mirrored:

```
storage aggregate show
```

O exemplo a seguir mostra que todos os agregados têm um status RAID espelhado:

```

cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster
      4.19TB      4.13TB   2% online    8 node_A_1  raid_dp,
mirrored,
normal

root_cluster
      715.5GB     212.7GB  70% online    1 node_A_1  raid4,
mirrored,
normal

cluster_B Switched Over Aggregates:
Aggregate Size      Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
data_cluster_B
      4.19TB      4.11TB   2% online    5 node_A_1  raid_dp,
mirrored,
normal

root_cluster_B    -          -        - unknown    - node_A_1  -

```

3. Nós de inicialização no local do desastre.
4. Verifique o status da recuperação de switchback:

```
metrocluster node show
```

```

cluster_A::> metrocluster node show
DR
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.

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.

A prática recomendada é que cada unidade de fonte de alimentação (PSU) de um componente seja conectada a uma fonte de alimentação separada. Se ambas as PSUs estiverem conectadas à mesma unidade de distribuição de energia (PDU) e ocorrer uma interrupção elétrica, o local pode ficar inativo e um compartimento completo pode ficar indisponível. A falha de uma linha de alimentação é testada para confirmar que não há incompatibilidade de cabeamento que possa causar uma interrupção do serviço.

Este teste deve levar cerca de 15 minutos.

Este teste requer a desativação da energia de todas as PDUs do lado esquerdo e, em seguida, de todas as PDUs do lado direito em todos os racks que contêm os componentes do MetroCluster.

Este procedimento tem os seguintes resultados esperados:

- Erros devem ser gerados à medida que as PDUs são desconetadas.
- Nenhum failover ou perda de serviço deve ocorrer.

Passos

1. Desligue a alimentação das PDUs no lado esquerdo do rack que contém os componentes MetroCluster.
2. Monitore o resultado no console usando os `system environment sensors show -state fault` comandos e `storage shelf show -errors`

```

cluster_A::> system environment sensors show -state fault

Node Sensor                State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
-----
node_A_1
    PSU1                    fault
                               PSU_OFF
    PSU1 Pwr In OK          fault
                               FAULT
node_A_2
    PSU1                    fault
                               PSU_OFF
    PSU1 Pwr In OK          fault
                               FAULT

4 entries were displayed.

cluster_A::> storage shelf show -errors
Shelf Name: 1.1
Shelf UID: 50:0a:09:80:03:6c:44:d5
Serial Number: SHFHU1443000059

Error Type                Description
-----
Power                      Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1

```

3. Ligue a alimentação novamente para as PDUs do lado esquerdo.
4. Certifique-se de que o ONTAP limpa a condição de erro.
5. Repita os passos anteriores com as PDUs do lado direito.

Verificação da operação após a perda de uma única prateleira de armazenamento

Você pode testar a falha de um único compartimento de storage para verificar se não há um ponto único de falha.

Este procedimento tem os seguintes resultados esperados:

- Uma mensagem de erro deve ser comunicada pelo software de monitorização.
- Nenhum failover ou perda de serviço deve ocorrer.
- A resincronização 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::> vservers show -type data
```

```
cluster_A::> vservers 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
```

```
storage aggregate show -r -node node_A_2 !*root
```

O agregado com unidades no compartimento desligado deve ter um status RAID "desclassificado" e as unidades no Plex afetado devem ter um status de "falha", como mostrado no exemplo a seguir:

```

cluster_A::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
-----

```

```

node_A_1data01_mirrored
      4.15TB      3.40TB      18% online      3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
      707.7GB      34.29GB      95% online      1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
      4.15TB      4.12TB      1% online      2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
      2.18TB      2.18TB      0% online      1 node_A_2
raid_dp,

normal
node_A_2_root
      707.7GB      34.27GB      95% online      1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)

Physical
      Position Disk
      Size Status
      -----

```

```

    dparity 2.30.3          0  BSAS  7200  827.7GB
828.0GB (normal)
    parity 2.30.4          0  BSAS  7200  827.7GB
828.0GB (normal)
    data 2.30.6            0  BSAS  7200  827.7GB
828.0GB (normal)
    data 2.30.8            0  BSAS  7200  827.7GB
828.0GB (normal)
    data 2.30.5            0  BSAS  7200  827.7GB
828.0GB (normal)

```

Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive, pool1)

RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none checksums)

					Usable
Physical					
Position	Disk	Pool	Type	RPM	Size
Size	Status				

dparity	FAILED	-	-	-	827.7GB
- (failed)					
parity	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					

Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block checksums)

Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active, pool0)

RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block checksums)

					Usable
Physical					
Position	Disk	Pool	Type	RPM	Size
Size	Status				

dparity	2.30.12	0	BSAS	7200	827.7GB
828.0GB	(normal)				

```
parity 2.30.22 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.21 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.20 0 BSAS 7200 827.7GB
828.0GB (normal)
data 2.30.14 0 BSAS 7200 827.7GB
828.0GB (normal)
```

15 entries were displayed.

7. Verifique se os dados estão sendo fornecidos e se todos os volumes ainda estão online:

```
vserver show -type data
```

```
network interface show -fields is-home false
```

```
volume show !vol0,!MDV*
```

```

cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
Admin      Operational Root
Vserver    Type      Subtype    State      State      Volume
Aggregate
-----
-----
SVM1       data      sync-source      running    SVM1_root
node_A_1_data01_mirrored
SVM2       data      sync-source      running    SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver    Volume      Aggregate    State      Type      Size
Available Used%
-----
-----
SVM1
          SVM1_root
                node_A_1data01_mirrored
                        online      RW      10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                node_A_1data01_mirrored
                        online      RW      10GB
9.49GB    5%
SVM2
          SVM2_root
                node_A_1data01_mirrored
                        online      RW      10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                node_A_2_data02_unmirrored
                        online      RW      1GB
972.6MB   5%

```

8. Ligue fisicamente a prateleira.

A resincronização 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

```

Conexões em configurações Stretch MetroCluster com LUNs de array

Conexões em configurações Stretch MetroCluster com LUNs de array

Em uma configuração Stretch MetroCluster, com LUNs de array, você precisa conectar as portas FC-VI entre controladores. Há suporte para conectividade direta entre os controladores e os storage arrays e-Series. Para todos os outros arrays de configurações

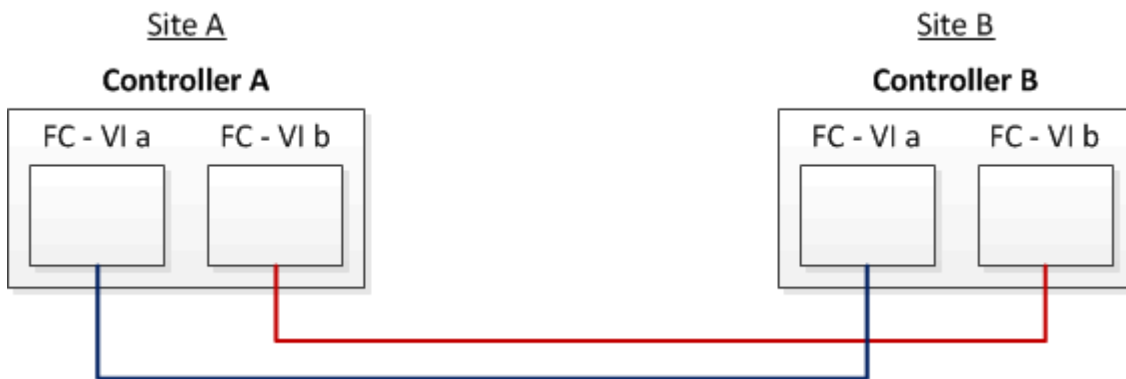
de LUN, você deve usar switches FC na configuração.

Você também pode configurar uma configuração Stretch MetroCluster com discos e LUNs de array. Em tal configuração, você precisa usar pontes FC para SAS ou cabos óticos SAS para conectar controladores a discos.

Exemplo de uma configuração Stretch MetroCluster com LUNs de array

Em uma configuração Stretch MetroCluster com LUNs de array, você precisa fazer o cabeamento das portas FC-VI para conectividade direta entre os controladores. Além disso, você deve fazer o cabeamento de cada porta HBA do controlador para alternar as portas nos switches FC correspondentes. O cabeamento das LUNs de array é igual ao de uma MetroCluster conectada à malha, com exceção das LUNs de array e-Series, que podem ser conectadas diretamente.

A ilustração a seguir mostra as portas FC-VI cabeadas entre os controladores A e B em uma configuração Stretch MetroCluster:



Os módulos dos controladores de sistemas de storage da FAS9000 usam quatro portas FC-VI cada uma.

Para configurações com LUNs de array e-Series, é possível conectar diretamente aos LUNs e-Series.

["Suporte de conexão direta para configuração Stretch MetroCluster com array NetApp e-Series"](#)

Com exceção da conexão das portas FC-VI, o restante deste procedimento é para a configuração de uma configuração MetroCluster com LUNs de array, que não estejam usando LUNs de array e-Series. Isso requer switches FC que são iguais ao uso de LUNs de array em configurações conectadas à malha.

["Instalação e configuração do MetroCluster conectado à malha"](#)

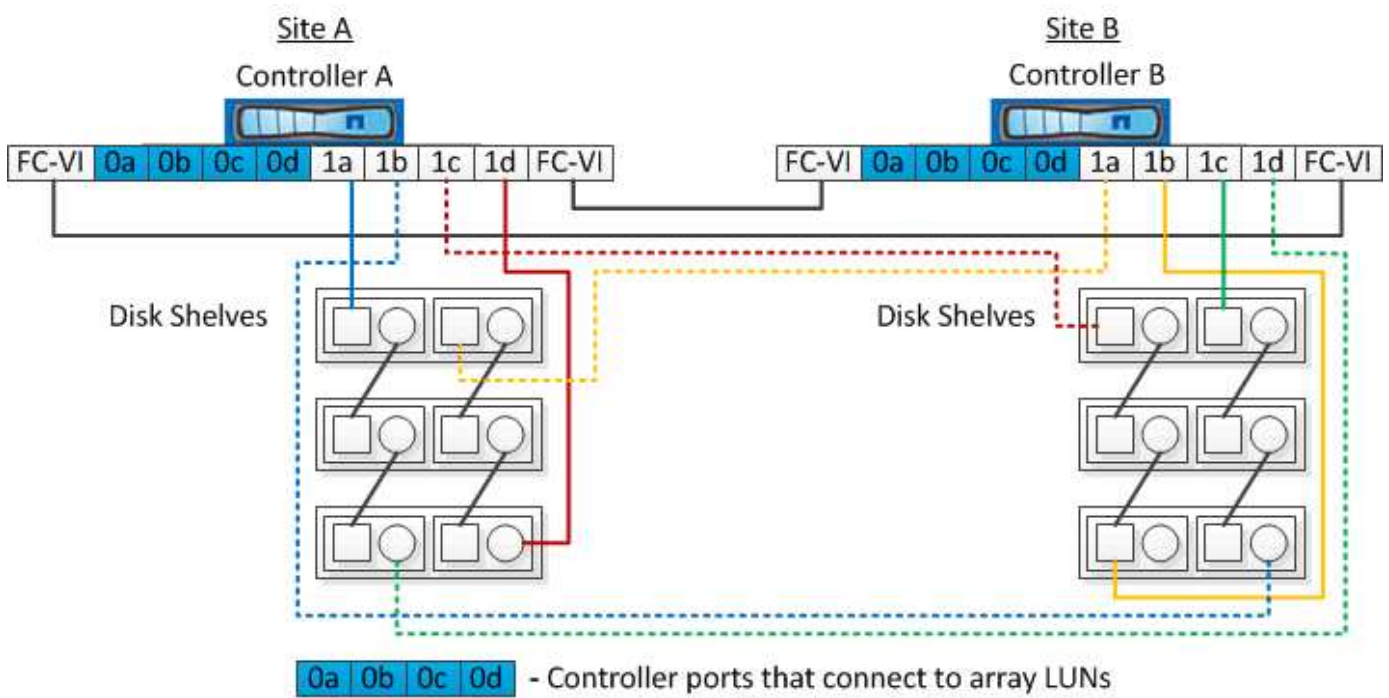
Exemplos de configurações Stretch MetroCluster de dois nós com discos e LUNs de array

Para configurar uma configuração Stretch MetroCluster com discos nativos e LUNs de array, você precisa usar pontes FC para SAS ou cabos óticos SAS para conectar os sistemas ONTAP às gavetas de disco. Além disso, os switches FC devem ser usados para conectar LUNs de array aos sistemas ONTAP.

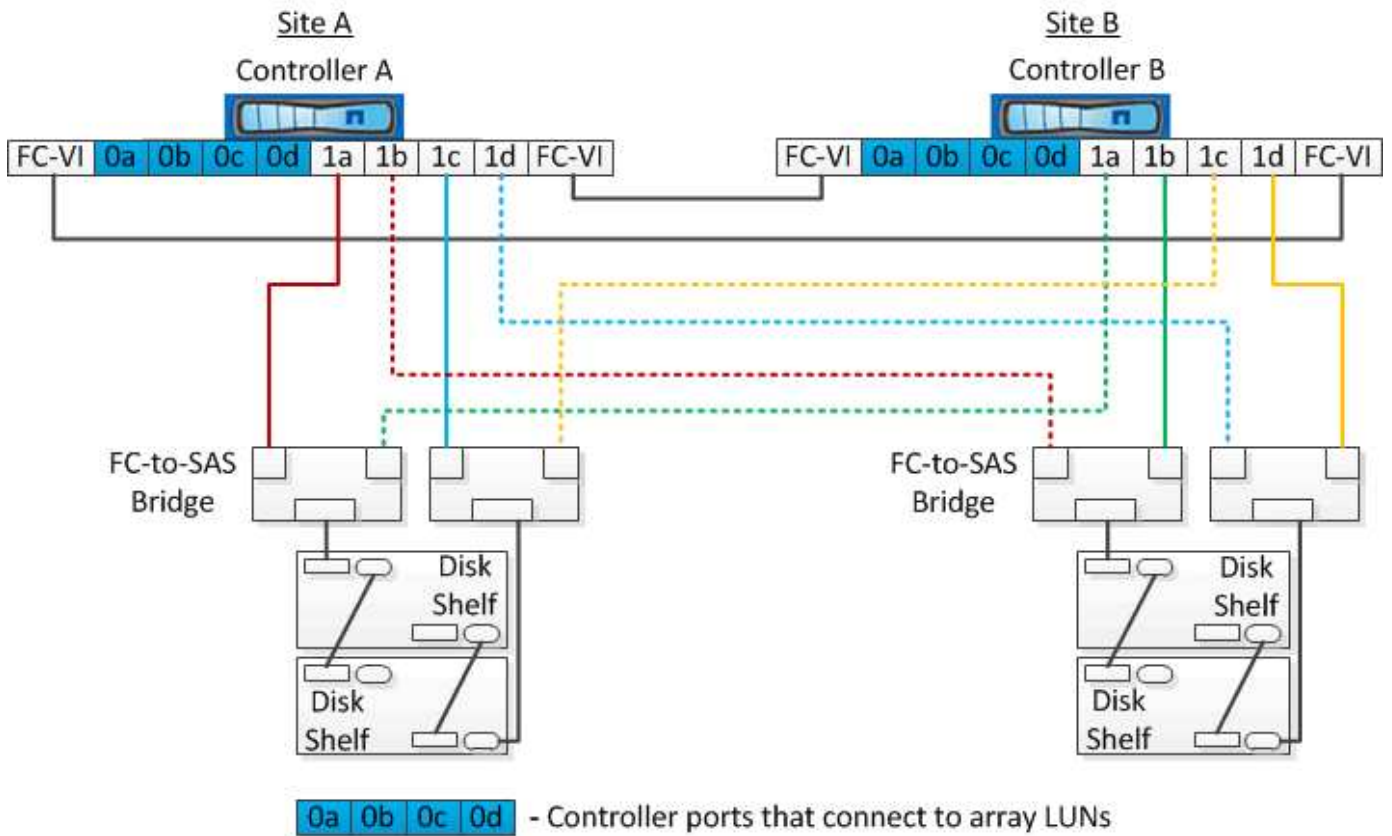
É necessário um mínimo de oito portas HBA para que um sistema ONTAP se conecte a discos nativos e LUNs de storage.

Nos exemplos a seguir que representam configurações de MetroCluster alongadas de dois nós com discos e LUNs de array, as portas HBA de 0a a 0d são usadas para conexão com LUNs de array. As portas HBA 1a a 1D são usadas para conexões com discos nativos.

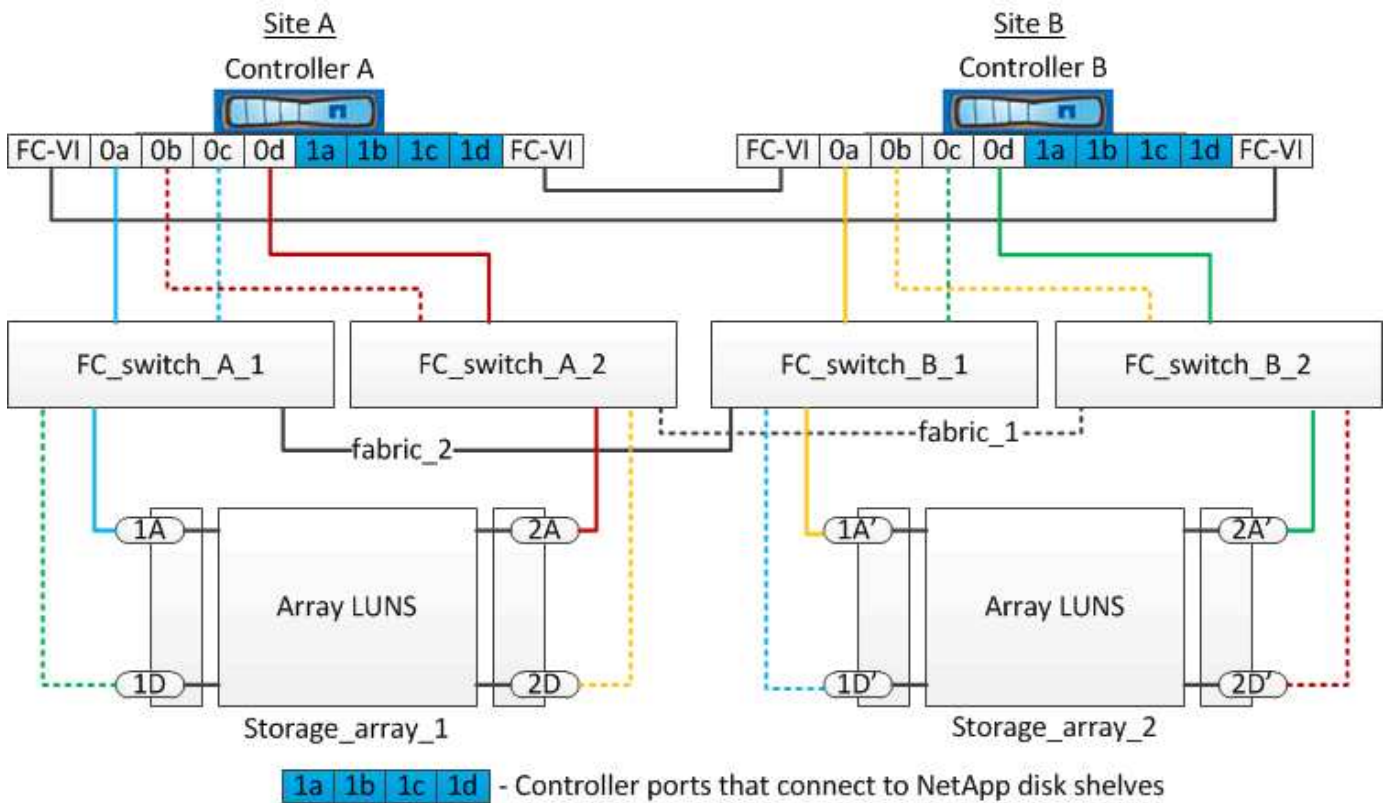
A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós na qual os discos nativos são conectados aos sistemas ONTAP usando cabos óticos SAS:



A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós na qual os discos nativos são conectados aos sistemas ONTAP usando bridges FC-para-SAS:



A ilustração a seguir mostra uma configuração Stretch MetroCluster de dois nós com as conexões LUN de array:





Se necessário, você também pode usar os mesmos switches FC para conectar discos nativos e LUNs de array às controladoras na configuração MetroCluster.

["Instalação e configuração do MetroCluster conectado à malha"](#)

Exemplo de uma configuração Stretch MetroCluster com storage arrays e-Series

Em uma configuração Stretch MetroCluster com um storage array LUNs e-Series, você pode conectar diretamente os controladores de armazenamento e os arrays de armazenamento. Ao contrário de outros LUNs de array, os switches FC não são necessários.

O ["Suporte de conexão direta para configuração Stretch MetroCluster com array NetApp e-Series"](#) artigo da base de conhecimento fornece exemplos de configurações com LUNs de array e-Series.

Considerações ao remover configurações do MetroCluster

Você pode remover a configuração do MetroCluster de todos os nós em um grupo de recuperação de desastres (DR). Depois de remover a configuração do MetroCluster, toda a 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."](#)

Como usar o Active IQ Unified Manager e o Gerenciador de sistemas ONTAP para configuração e monitoramento adicionais

Uso do Active IQ Unified Manager e do Gerenciador de sistemas do ONTAP para configuração e monitoramento adicionais

O Active IQ Unified Manager e o ONTAP System Manager podem ser usados para o gerenciamento de GUI dos clusters e para o monitoramento da configuração.

Cada nó tem o Gerenciador de sistema do ONTAP pré-instalado. Para carregar o System Manager, insira o endereço LIF de gerenciamento de cluster como URL em um navegador da Web que tem conectividade com o nó.

Você também pode usar o Active IQ Unified Manager para monitorar a configuração do MetroCluster.

Informações relacionadas

["Documentação do Gestor de sistemas Active IQ Unified Manager e ONTAP"](#)

Sincronizar a hora do sistema usando NTP

Cada cluster precisa de seu próprio servidor NTP (Network Time Protocol) para sincronizar o tempo entre os nós e seus clientes. Você pode usar a caixa de diálogo Editar DateTime no System Manager para configurar o servidor NTP.

Verifique se você baixou e instalou o System Manager. O Gerenciador do sistema está disponível no site de suporte da NetApp.

- Não é possível modificar as configurações de fuso horário para um nó com falha ou para o nó do parceiro após a aquisição ocorrer.
- Cada cluster na configuração do MetroCluster FC deve ter seu próprio servidor NTP separado ou servidores usados pelos nós e (se houver) pontes FC para SAS nesse local do MetroCluster.

Se você estiver usando o software tiebreaker do MetroCluster, ele também deve ter seu próprio servidor NTP separado.

Passos

1. Na página inicial, clique duas vezes no sistema de armazenamento apropriado.
2. Expanda a hierarquia **Cluster** no painel de navegação esquerdo.
3. No painel de navegação, clique em **Configuração > Ferramentas do sistema > DateTime**.
4. Clique em **Editar**.
5. Selecione o fuso horário.
6. Especifique os endereços IP dos servidores de hora e clique em **Adicionar**.

Você deve adicionar um servidor NTP à lista de servidores de hora. O controlador de domínio pode ser um servidor autorizado.

7. Clique em **OK**.
8. Verifique as alterações feitas nas configurações de data e hora na janela Data e hora.

Considerações ao usar o ONTAP em uma configuração do MetroCluster

Ao usar o ONTAP em uma configuração do MetroCluster, você deve estar ciente de certas considerações sobre licenciamento, peering para clusters fora da configuração do MetroCluster, execução de operações de volume, operações NVFAIL e outras operações do ONTAP.

Considerações sobre licenciamento

- Ambos os sites devem ser licenciados para os mesmos recursos licenciados pelo site.
- Todos os nós devem ser licenciados para os mesmos recursos de bloqueio de nó.

Consideração de SnapMirror

- A recuperação de desastres do SnapMirror SVM só é compatível com configurações do MetroCluster

executando versões do ONTAP 9.5 ou posterior.

Suporte FlexCache em uma configuração MetroCluster

A partir do ONTAP 9.7, os volumes FlexCache são compatíveis com configurações do MetroCluster. Você deve estar ciente dos requisitos para a repetibilidade manual após operações de comutação ou switchback.

Repetibilidade da SVM após o switchover quando a origem e o cache do FlexCache estão no mesmo local do MetroCluster

Após um switchover negociado ou não planejado, qualquer relacionamento de peering SVM FlexCache no cluster deve ser configurado manualmente.

Por exemplo, svms VS1 (cache) e VS2 (origem) estão no site_A. Esses SVMs são peered.

Após o switchover, os svms VS1-MC e VS2-mc são ativados no local do parceiro (site_B). Eles devem ser manualmente repelidos para que o FlexCache funcione usando o `vserver peer repeer` comando.

Repetibilidade da SVM após switchover ou switchback quando um destino FlexCache está em um terceiro cluster e no modo desconetado

Para as relações do FlexCache com um cluster fora da configuração do MetroCluster, o peering deve ser sempre reconfigurado manualmente após um switchover quando os clusters envolvidos estão em um modo desconetado durante o switchover.

Por exemplo:

- Um fim do FlexCache (cache_1 no VS1) reside no MetroCluster site_A tem um fim do FlexCache
- A outra extremidade do FlexCache (origin_1 no VS2) reside no site_C (não na configuração do MetroCluster)

Quando o switchover é acionado e se o site_A e o site_C não estiverem 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.

Suporte FabricPool em configurações MetroCluster

A partir do ONTAP 9.7, as configurações do MetroCluster são compatíveis com camadas de storage FabricPool.

Para obter informações gerais sobre como usar o FabricPools, consulte "[Gerenciamento de discos e agregados](#)".

Considerações ao usar FabricPools

- Os clusters precisam ter licenças FabricPool com limites de capacidade correspondentes.
- Os clusters devem ter IPspaces com nomes correspondentes.

Esse pode ser o espaço IPspace padrão ou um espaço IP criado por um administrador. Este espaço IPspace será usado para configurações de armazenamento de objetos FabricPool.

- Para o espaço IPspace selecionado, cada cluster deve ter um LIF entre clusters definido que possa alcançar o armazenamento de objetos externo

Configurando um agregado para uso em um FabricPool espelhado



Antes de configurar o agregado, você deve configurar armazenamentos de objetos conforme descrito em "Configurando armazenamentos de objetos para FabricPool em uma configuração MetroCluster" no "[Gerenciamento de discos e agregados](#)".

Para configurar um agregado para uso em um FabricPool:

1. Crie o agregado ou selecione um agregado existente.
2. Espelhe o agregado como um agregado espelhado típico na configuração do MetroCluster.
3. Crie o espelho FabricPool com o agregado, conforme descrito no "[Gerenciamento de discos e agregados](#)":
 - a. Anexe um armazenamento de objetos primário.

Este armazenamento de objetos está fisicamente mais perto do cluster.

- b. Adicione um armazenamento de objetos espelhados.

Este armazenamento de objetos está fisicamente mais longe do cluster do que o armazenamento de objetos principal.

Suporte FlexGroup em configurações MetroCluster

A partir do ONTAP 9.6, as configurações do MetroCluster são compatíveis com volumes FlexGroup.

Programações de trabalhos em uma configuração MetroCluster

No ONTAP 9.3 e posterior, as programações de tarefas criadas pelo usuário são replicadas automaticamente entre clusters em uma configuração do MetroCluster. Se você criar, modificar ou excluir um agendamento de trabalho em um cluster, o mesmo agendamento será criado automaticamente no cluster de parceiros, usando o CRS (Configuration Replication Service).



As programações criadas pelo sistema não são replicadas e você deve executar manualmente a mesma operação no cluster de parceiros para que as programações de tarefas em ambos os clusters sejam idênticas.

Peering de cluster do site MetroCluster para um terceiro cluster

Como a configuração de peering não é replicada, se você identificar um dos clusters na configuração do MetroCluster para um terceiro cluster fora dessa configuração, você também deverá configurar o peering no cluster do MetroCluster parceiro. Isso é para que o peering possa ser mantido se ocorrer um switchover.

O cluster que não é MetroCluster deve estar executando o ONTAP 8,3 ou posterior. Caso contrário, o peering é perdido se ocorrer um switchover, mesmo que o peering tenha sido configurado em ambos os parceiros da MetroCluster.

Replicação de configuração de cliente LDAP em uma configuração MetroCluster

Uma configuração de cliente LDAP criada em uma máquina virtual de storage (SVM) em um cluster local é replicada para os dados de parceiros SVM no cluster remoto. Por exemplo, se a configuração do cliente LDAP for criada no SVM admin no cluster local, ela será replicada para todos os SVMs de dados administrativos no cluster remoto. Esse recurso do MetroCluster é intencional para que a configuração do cliente LDAP esteja ativa em todos os SVMs de parceiros no cluster remoto.

Diretrizes de criação de LIF e rede para configurações do MetroCluster

Você deve estar ciente de como LIFs são criados e replicados em uma configuração do MetroCluster. Você também deve saber sobre o requisito de consistência para que você possa tomar as decisões adequadas ao configurar sua rede.

Informações relacionadas

["Conceitos de ONTAP"](#)

Requisitos de replicação de objeto IPspace e configuração de sub-rede

Você deve estar ciente dos requisitos para replicar objetos IPspace no cluster de parceiros e para configurar sub-redes e IPv6 em uma configuração do MetroCluster.

Replicação IPspace

Você deve considerar as diretrizes a seguir enquanto replica objetos IPspace para o cluster de parceiros:

- Os nomes de IPspace dos dois locais devem corresponder.
- Os objetos IPspace devem ser replicados manualmente para o cluster do parceiro.

Quaisquer máquinas virtuais de armazenamento (SVMs) que sejam criadas e atribuídas a um IPspace antes que o IPspace seja replicado não serão replicadas para o cluster de parceiros.

Configuração de sub-rede

Você deve considerar as seguintes diretrizes ao configurar sub-redes em uma configuração do MetroCluster:

- Ambos os clusters da configuração do MetroCluster devem ter uma sub-rede no mesmo espaço IPspace com o mesmo nome de sub-rede, sub-rede, domínio de broadcast e gateway.
- Os intervalos de IP dos dois clusters devem ser diferentes.

No exemplo a seguir, os intervalos de IP são diferentes:

```
cluster_A::> network subnet show
```

```
IPspace: Default
```

Subnet	Broadcast	Avail/			
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
	192.168.2.11-192.168.2.20				

```
cluster_B::> network subnet show
```

```
IPspace: Default
```

Subnet	Broadcast	Avail/			
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
	192.168.2.21-192.168.2.30				

Configuração IPv6

Se o IPv6 estiver configurado em um site, o IPv6 também deve ser configurado no outro site.

Requisitos para criação de LIF em uma configuração MetroCluster

Você deve estar ciente dos requisitos para criar LIFs ao configurar sua rede em uma configuração do MetroCluster.

Você deve considerar as seguintes diretrizes ao criar LIFs:

- Fibre Channel: Você precisa usar VSAN esticada ou tecidos esticados.
- IP/iSCSI: Você deve usar a rede estendida da camada 2.
- Broadcasts ARP: Você deve habilitar broadcasts ARP entre os dois clusters.
- LIFs duplicadas: Você não deve criar vários LIFs com o mesmo endereço IP (LIFs duplicadas) em um espaço IPspace.
- Configurações NFS e SAN: Você precisa usar diferentes máquinas virtuais de storage (SVMs) para agregados sem espelhamento e espelhados.
- Você deve criar um objeto de sub-rede antes de criar um LIF. Um objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque tem um domínio de broadcast associado.

Verifique a criação de LIF

Você pode confirmar a criação bem-sucedida de um LIF em uma configuração do MetroCluster executando o `metrocluster check lif show` comando. Se você encontrar algum problema ao criar o LIF, você pode usar o `metrocluster check lif repair-placement` comando para corrigir os problemas.

Requisitos e problemas de replicação e posicionamento de LIF

Você deve estar ciente dos requisitos de replicação do LIF em uma configuração do MetroCluster. Você também deve saber como um LIF replicado é colocado em um cluster de parceiros e estar ciente dos problemas que ocorrem quando a replicação LIF ou o posicionamento de LIF falha.

Replicação de LIFs para o cluster de parceiros

Quando você cria um LIF em um cluster em uma configuração do MetroCluster, o LIF é replicado no cluster de parceiros. LIFs não são colocados em uma base de nome individual. Para disponibilidade de LIFs após uma operação de switchover, o processo de colocação de LIF verifica se as portas são capazes de hospedar o LIF com base em verificações de acessibilidade e atributos de porta.

O sistema deve atender às seguintes condições para colocar as LIFs replicadas no cluster de parceiros:

Condição	Tipo de LIF: FC	Tipo de LIF: IP/iSCSI
Identificação do nó	<p>O ONTAP tenta colocar o LIF replicado no parceiro de recuperação de desastres (DR) do nó no qual ele foi criado.</p> <p>Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.</p>	<p>O ONTAP tenta colocar o LIF replicado no parceiro de DR do nó no qual ele foi criado.</p> <p>Se o parceiro de DR não estiver disponível, o parceiro auxiliar de DR será usado para colocação.</p>
Identificação da porta	<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 conectada 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>

Colocação de LIF	A partir das portas alcançáveis, o ONTAP seleciona a porta menos carregada para colocação.	A partir das portas selecionadas, o ONTAP seleciona a porta menos carregada para colocação.
------------------	--	---

Colocação de LIFs replicadas quando o nó do parceiro de DR está inativo

Quando um iSCSI ou FC LIF é criado em um nó cujo parceiro de DR foi assumido, o LIF replicado é colocado no nó do parceiro auxiliar de DR. Após uma operação subsequente de giveback, os LIFs não são movidos automaticamente para o parceiro DR. Isso pode levar a que os LIFs se concentrem em um único nó no cluster de parceiros. Durante uma operação de switchover do MetroCluster, tentativas subsequentes de mapear LUNs pertencentes à máquina virtual de storage (SVM) falham.

Você deve executar o `metrocluster check lif show` comando após uma operação de aquisição ou operação de giveback para verificar se o posicionamento de LIF está correto. Se existirem erros, pode executar o `metrocluster check lif repair-placement` comando para resolver os problemas.

Erros de colocação de LIF

Os erros de colocação de LIF que são exibidos pelo `metrocluster check lif show` comando são retidos após uma operação de comutação. Se o `network interface modify` comando, `network interface rename` ou `network interface delete` for emitido para um LIF com um erro de posicionamento, o erro será removido e não aparecerá na saída do `metrocluster check lif show` comando.

Falha de replicação de LIF

Você também pode verificar se a replicação do LIF foi bem-sucedida usando o `metrocluster check lif show` comando. Uma mensagem EMS é exibida se a replicação LIF falhar.

Você pode corrigir uma falha de replicação executando o `metrocluster check lif repair-placement` comando para qualquer LIF que não consiga encontrar uma porta correta. Você deve resolver quaisquer falhas de replicação de LIF o mais rápido possível para verificar a disponibilidade de LIF durante uma operação de switchover de MetroCluster.



Mesmo que o SVM de origem esteja inativo, o posicionamento de LIF pode continuar normalmente se houver um LIF pertencente a um SVM diferente em uma porta com o mesmo espaço IPspace e rede no SVM de destino.

Criação de volume em um agregado raiz

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

Devido a essa restrição, os agregados de raiz não podem ser adicionados a um SVM usando o `vserver add-aggregates` comando.

Recuperação de desastres do SVM em uma configuração de MetroCluster

A partir do ONTAP 9.5, as máquinas virtuais de storage ativo (SVMs) em uma configuração do MetroCluster podem ser usadas como fontes com o recurso de recuperação de desastres do SnapMirror SVM. O SVM de destino deve estar no terceiro cluster fora da configuração do MetroCluster.

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

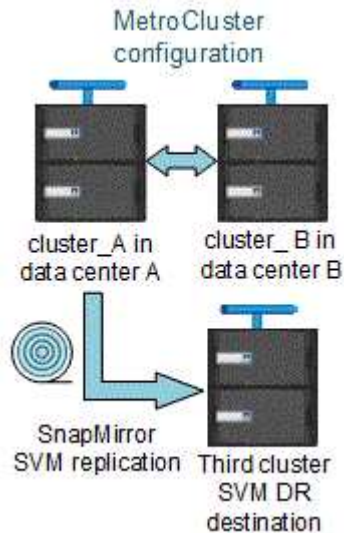
do SnapMirror:

- Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM.

Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover.

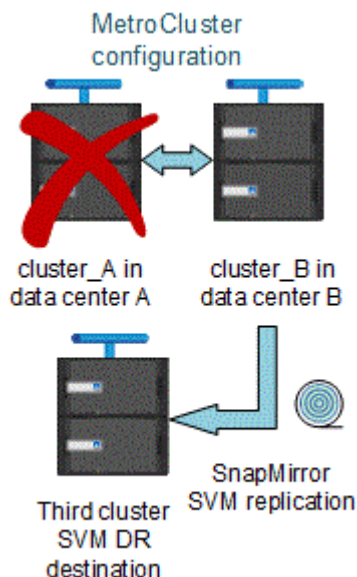
- Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online.

A imagem a seguir mostra o comportamento de recuperação de desastres do SVM em um estado estável:



- Quando o SVM de origem sincronizada é a fonte de uma relação SVM DR, as informações de origem no relacionamento de SVM DR são replicadas para o parceiro MetroCluster.

Isso permite que as atualizações do SVM DR continuem após um switchover, conforme mostrado na imagem a seguir:



- Durante os processos de switchover e switchback, a replicação para o destino SVM DR pode falhar.

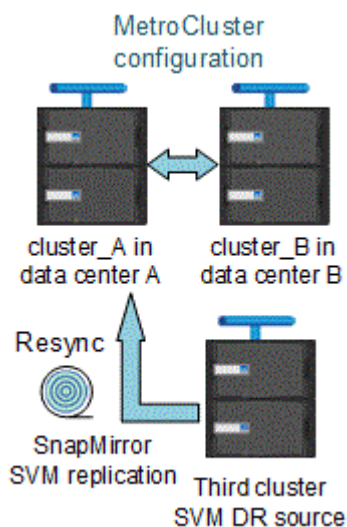
No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas do SVM DR serão bem-sucedidas.

Consulte a seção ""replicando a configuração do SVM"" no ["Proteção de dados com a CLI"](#) para obter detalhes sobre como configurar um relacionamento de DR do SVM.

Ressincronização da SVM em um local de recuperação de desastre

Durante a ressincronização, a fonte de recuperação de desastres (DR) de máquinas virtuais de storage (SVMs) na configuração MetroCluster é restaurada a partir do SVM de destino no local que não é MetroCluster.

Durante a ressincronização, o SVM de origem (cluster_A) atua temporariamente como SVM de destino, conforme mostrado na imagem a seguir:



Se um switchover não planejado ocorrer durante a ressincronização

Switchovers não planejados que ocorrem durante a ressincronização interromperão a transferência de ressincronização. Se ocorrer um switchover não planejado, as seguintes condições são verdadeiras:

- O SVM de destino no local do MetroCluster (que era uma fonte SVM antes da ressincronização) permanece como um SVM de destino. O SVM no cluster de parceiros continuará mantendo seu subtipo e inativo.
- A relação do SnapMirror deve ser recriada manualmente com o SVM de destino de sincronização como destino.
- A relação SnapMirror não aparece na saída do show do SnapMirror após um switchover no local sobrevivente, a menos que uma operação de criação do SnapMirror seja executada.

Execução do switchback após um switchover não planejado durante a ressincronização

Para executar com sucesso o processo de switchback, a relação de ressincronização deve ser quebrada e excluída. O switchback não é permitido se houver algum SVMs de destino de DR do SnapMirror na configuração do MetroCluster ou se o cluster tiver um SVM de subtipo "dp-destination".

Saída dos comandos `show de disco de armazenamento e shelf de armazenamento show` em uma configuração `Stretch MetroCluster` de dois nós

Em uma configuração `Stretch MetroCluster` de dois nós, `is-local-attach` o campo dos `storage disk show` comandos e `storage shelf show` mostra todos os discos e compartimentos de `storage` como locais, independentemente do nó ao qual eles estão conectados.

A saída para o comando `storage Aggregate plex show` é indeterminada após um `switchover` do `MetroCluster`

Quando você executa o `storage aggregate plex show` comando após um `switchover` do `MetroCluster`, o status de `plex0` do agregado de raiz comutada é indeterminado e é exibido como `failed`. Durante este tempo, a raiz comutada não é atualizada. O estado real deste `Plex` só pode ser determinado após a fase de cicatrização do `MetroCluster`.

Modificação de volumes para definir o sinalizador `NVFAIL` em caso de comutação

Você pode modificar um volume para que o sinalizador `NVFAIL` seja definido no volume em caso de um `switchover` `MetroCluster`. O sinalizador `NVFAIL` faz com que o volume seja vedado de qualquer modificação. Isso é necessário para volumes que precisam ser tratados como se as gravações confirmadas no volume fossem perdidas após o `switchover`.



Nas versões do `ONTAP` anteriores a 9,0, o sinalizador `NVFAIL` é usado para cada `switchover`. No `ONTAP 9.0` e versões posteriores, o `switchover` não planejado (`USO`) é usado.

Passos

1. Ative a configuração do `MetroCluster` para acionar o `NVFAIL` no `switchover` definindo o `vol -dr-force -nvfail` parâmetro como `"on"`:

```
vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
```

Transição de uma configuração `MetroCluster` elástica para uma configuração de malha

Em uma configuração `MetroCluster` conectada à malha, os nós estão em diferentes locais. Essa diferença geográfica aumenta a proteção contra desastres. Para fazer a transição de uma configuração `Stretch` para uma `MetroCluster` conectada à malha, é necessário adicionar switches `FC` e, se necessário, pontes `FC` para `SAS` à configuração.

- Você deve desativar o `switchover` automático em ambos os clusters executando o `metrocluster modify -auto-switchover-failure-domain auto-disabled` comando.
- Você precisa ter encerrado os nós.

Este procedimento é disruptivo.

A configuração do `MetroCluster` deve ser transferida em ambos os sites. Após atualizar a configuração do `MetroCluster`, você precisa habilitar o `switchover` automático nos dois clusters. Também é necessário validar a configuração executando o `metrocluster check run` comando.

Este procedimento fornece uma visão geral dos passos necessários. Para obter instruções detalhadas, consulte as seções específicas do ["Instalação e configuração do MetroCluster conectado à malha"](#). Você não precisa fazer uma instalação e configuração completas.

Passos

1. Prepare-se para a atualização revisando cuidadosamente a seção "preparação para a instalação do MetroCluster" do ["Instalação e configuração do MetroCluster conectado à malha"](#).
2. Instale, faça cabos e configure os switches e as bridges FC-para-SAS necessários.



Você deve usar os procedimentos na seção "cabramento de uma configuração de MetroCluster conetada à malha" do ["Instalação e configuração do MetroCluster conectado à malha"](#).

3. Atualize a configuração do MetroCluster usando as etapas a seguir.

Não use os procedimentos na seção "Configurando o software MetroCluster no ONTAP" localizada no ["Instalação e configuração do MetroCluster conectado à malha"](#).

- a. Entre no modo de privilégio avançado `set -privilege advanced`
- b. Atualize a configuração do MetroCluster `metrocluster configure -refresh true`

O comando a seguir atualiza a configuração do MetroCluster em todos os nós do grupo DR que contém controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

- a. Voltar ao modo de privilégio de administrador `set -privilege admin`

4. Verifique se há erros na configuração do MetroCluster e verifique se ela está operacional.

Você deve usar os procedimentos nas seções a seguir do ["Instalação e configuração do MetroCluster conectado à malha"](#):

- Verificando erros de configuração do MetroCluster com o Config Advisor
- Verificação da operação local de HA
- Verificando switchover, cura e switchback

Onde encontrar informações adicionais

Você pode saber mais sobre a configuração e operação do MetroCluster.

MetroCluster e informações diversas

Informações	Assunto
"Documentação do ONTAP 9"	<ul style="list-style-type: none">• Todos os guias MetroCluster

	<ul style="list-style-type: none"> • Uma visão geral técnica da configuração e operação do MetroCluster FC. • Práticas recomendadas para configuração MetroCluster FC.
"Instalação e configuração do MetroCluster conectado à malha"	<ul style="list-style-type: none"> • Arquitetura MetroCluster conectada à malha • Fazer o cabeamento da configuração • Configuração de pontes FC para SAS • Configuração dos switches FC • Configurando o MetroCluster no ONTAP
"Instalação e configuração do IP MetroCluster: Diferenças entre as configurações do ONTAP MetroCluster"	<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 (DR)
"Mantenha os componentes do MetroCluster"	<ul style="list-style-type: none"> • Diretrizes para manutenção em uma configuração MetroCluster FC • Substituição ou atualização de hardware. Procedimentos de atualização de firmware para bridges FC para SAS e switches FC • Adição automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Remoção automática de um compartimento de disco em uma configuração MetroCluster FC elástica ou conectada à malha • Substituição do hardware em um local de recuperação de desastres em uma configuração MetroCluster FC estendida ou conectada à malha • Expansão de uma configuração Stretch MetroCluster FC ou conectada à malha de dois nós para uma configuração MetroCluster de quatro nós. • Expansão de uma configuração de MetroCluster FC elástica ou conectada à malha de quatro nós para uma configuração de MetroCluster FC de oito nós.

<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 Active IQ Unified Manager</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.