



Configure os componentes de hardware do MetroCluster

ONTAP MetroCluster

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/ontap-metrocluster/install-ip/concept_parts_of_an_ip_mcc_configuration_mcc_ip.html on February 13, 2026. Always check docs.netapp.com for the latest.

Índice

Configure os componentes de hardware do MetroCluster	1
Aprenda sobre interconexões de componentes de hardware em uma configuração de IP do MetroCluster	1
Principais elementos de hardware	1
Grupos de recuperação de desastres (DR)	2
Ilustração dos pares de HA locais em uma configuração do MetroCluster	2
Ilustração da rede de interligação de cluster e IP MetroCluster	3
Ilustração da rede de peering de cluster	4
Componentes de configuração de IP do MetroCluster necessários e convenções de nomenclatura	5
Software e hardware suportados	5
Requisitos de redundância de hardware em uma configuração IP MetroCluster	5
Requisitos de cluster do ONTAP em uma configuração IP do MetroCluster	6
Requisitos de switch IP em uma configuração IP MetroCluster	6
Requisitos do módulo do controlador em uma configuração IP do MetroCluster	6
Requisitos de adaptador Gigabit Ethernet em uma configuração IP MetroCluster	7
Requisitos de pool e unidade (mínimo suportado)	8
Considerações sobre o local da unidade para compartimentos parcialmente preenchidos	9
Considerações sobre o local da unidade para unidades internas AFF A800	9
Componentes de hardware de configuração do MetroCluster IP	9
Cable os switches IP MetroCluster	10
Como usar as tabelas de portas com várias configurações de IP do MetroCluster	10
Atribuições de portas de plataforma para switches Cisco 3132Q-V em uma configuração IP MetroCluster	11
Atribuições de porta de plataforma para switches Cisco 3232C ou Cisco 9336C de 36 portas em uma configuração IP MetroCluster	14
Atribuições de portas de plataforma para switches Cisco 9336C-FX2 de 12 portas em uma configuração IP MetroCluster	25
Atribuições de porta de plataforma para um switch Cisco 9336C-FX2 de 36 portas conectando armazenamento NS224 em uma configuração IP MetroCluster	33
Atribuições de porta de plataforma para switches IP BES-53248 com suporte da Broadcom em uma configuração IP MetroCluster	48
Atribuições de porta de plataforma para switches IP SN2100 com suporte da NVIDIA em uma configuração IP MetroCluster	55
Cabear as portas do módulo controlador ONTAP em uma configuração IP do MetroCluster	60
Configure os switches IP MetroCluster	61
Escolha o procedimento correto de configuração do switch IP do MetroCluster	61
Configurar switches IP Broadcom para interconexão de cluster e conectividade IP MetroCluster de backend	61
Configurar switches IP Cisco	80
Configurar switches IP NVIDIA	102
Monitorar a integridade do switch IP do MetroCluster	118
Saiba mais sobre o monitoramento da integridade do switch em uma configuração de IP do MetroCluster	118

Configurar SNMPv3 para monitorar a integridade dos switches IP do MetroCluster	118
Configurar coleta de logs em um switch IP do MetroCluster	136
Gerenciar o monitoramento de switches Ethernet em uma configuração IP do MetroCluster	143
Verificar o monitoramento do switch Ethernet em uma configuração de IP do MetroCluster	144

Configure os componentes de hardware do MetroCluster

Aprenda sobre interconexões de componentes de hardware em uma configuração de IP do MetroCluster

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

Principais elementos de hardware

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

- Controladores de storage

As controladoras de storage são configuradas como dois clusters de dois nós.

- Rede IP

Esta rede IP back-end fornece conectividade para dois usos distintos:

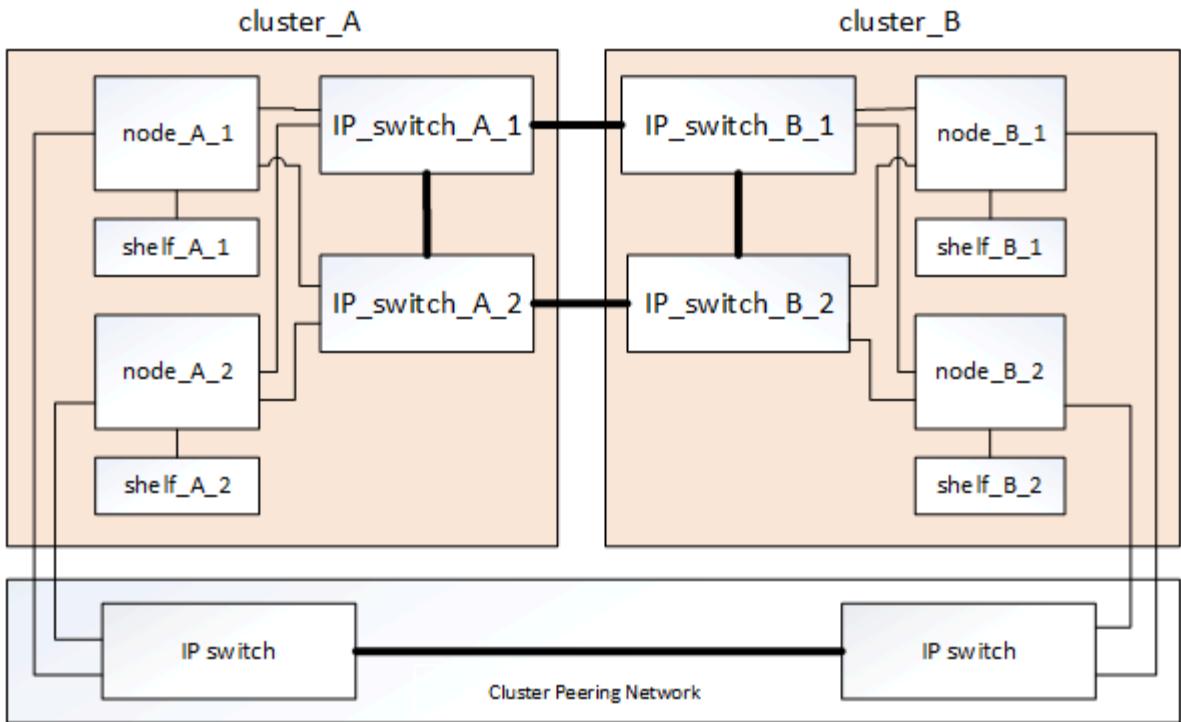
- Conectividade de cluster padrão para comunicações intra-cluster.

Essa é a mesma funcionalidade de switch de cluster usada em clusters ONTAP não comutados da MetroCluster.

- Conectividade de back-end MetroCluster para replicação de dados de storage e cache não volátil.

- Rede de peering de cluster

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



Grupos de recuperação de desastres (DR)

Uma configuração IP do MetroCluster consiste em um grupo de DR de quatro nós.

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

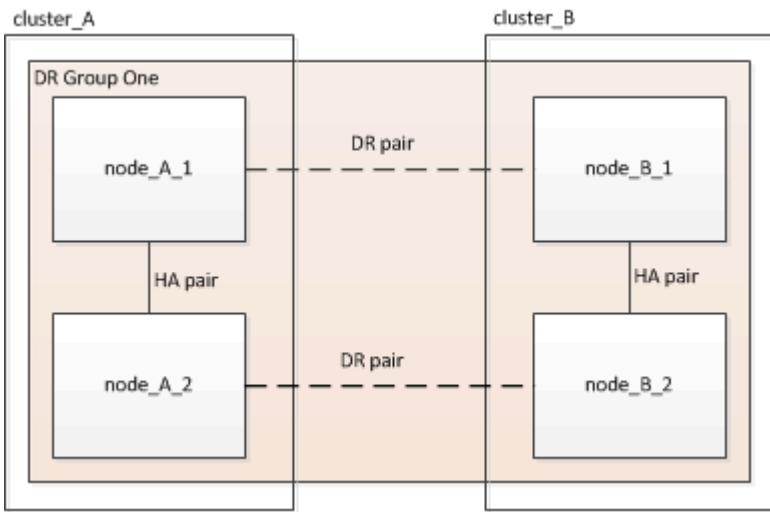
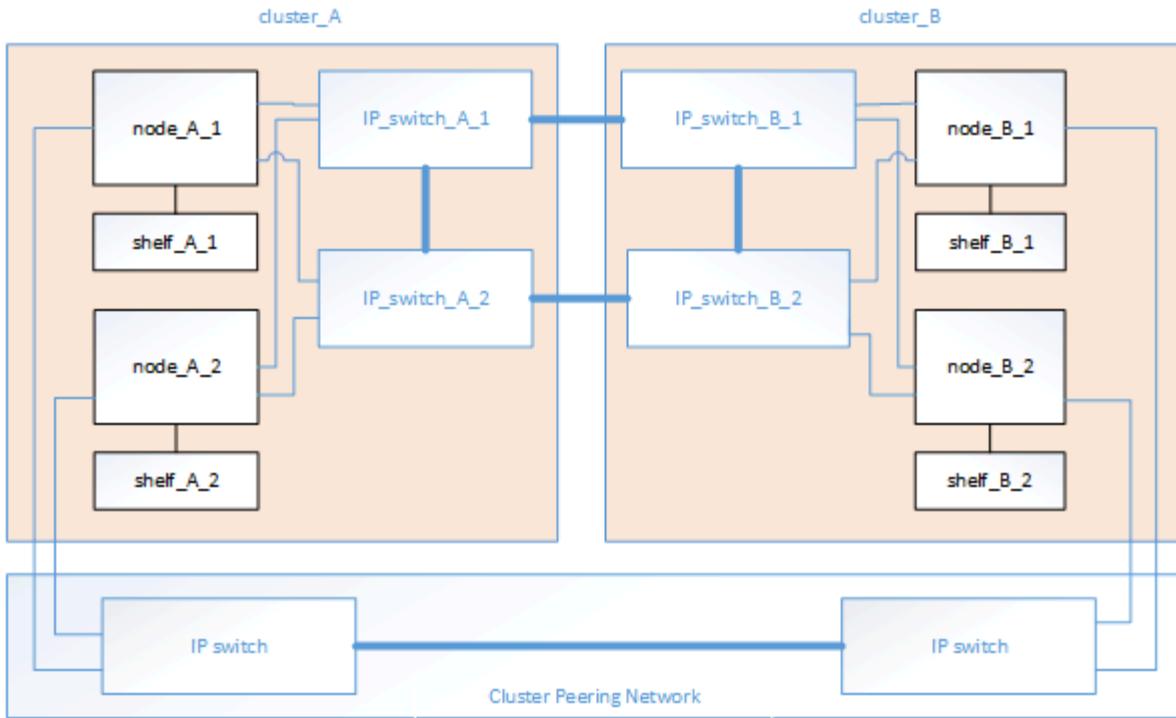


Ilustração dos pares de HA locais em uma configuração do MetroCluster

Cada local do MetroCluster consiste em controladores de storage configurados como um par de HA. Isso permite redundância local para que, se um controlador de storage falhar, seu parceiro de HA local possa assumir o controle. Essas falhas podem ser tratadas sem uma operação de switchover do MetroCluster.

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

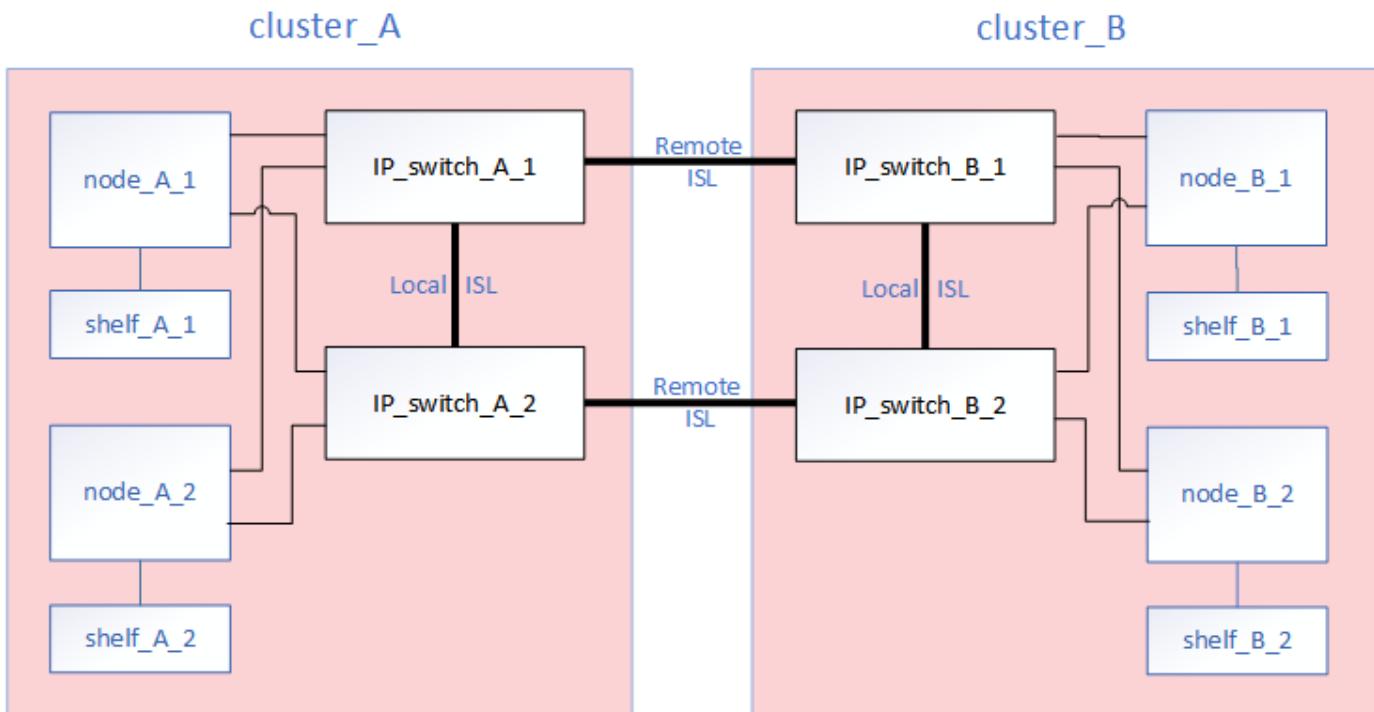


Informações relacionadas

["Conceitos de ONTAP"](#)

Ilustração da rede de interligação de cluster e IP MetroCluster

Os clusters do ONTAP geralmente incluem uma rede de interconexão de cluster para tráfego entre os nós no cluster. Nas configurações IP do MetroCluster, essa rede também é usada para transportar tráfego de replicação de dados entre os sites do MetroCluster.

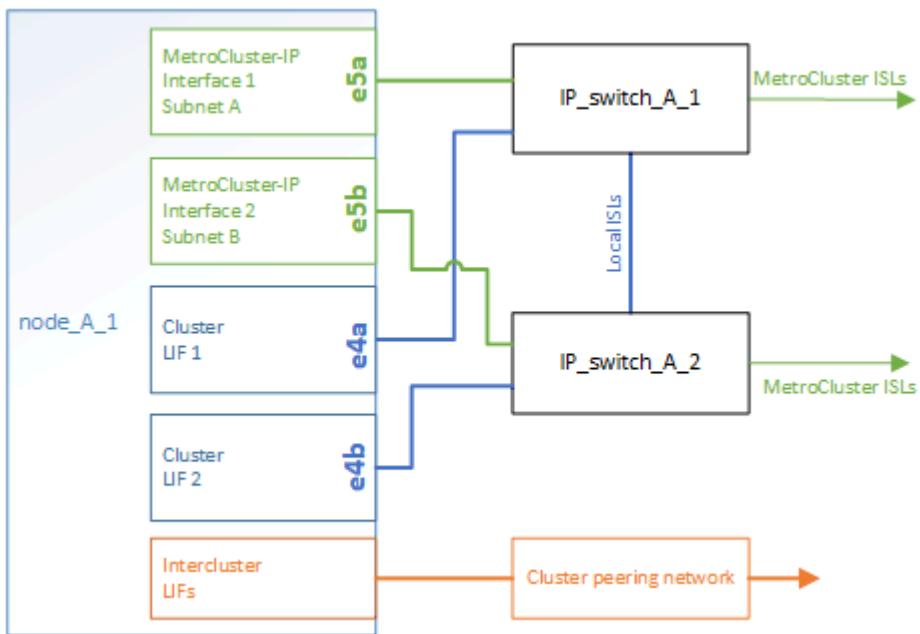


Cada nó na configuração IP do MetroCluster tem interfaces dedicadas para conexão com a rede IP de back-

end:

- Duas interfaces IP MetroCluster
- Duas interfaces de cluster locais

A ilustração a seguir mostra essas interfaces. O uso da porta mostrado é para um sistema AFF A700 ou FAS9000.



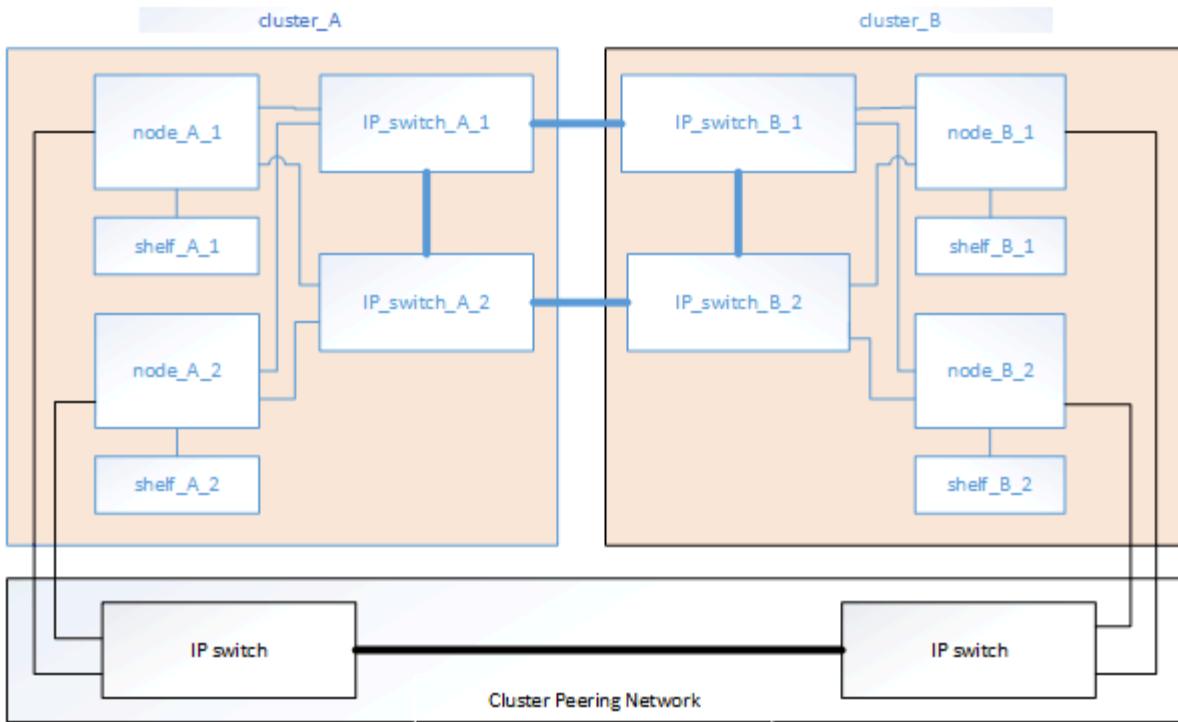
Informações relacionadas

["Considerações para configurações IP do MetroCluster"](#)

Ilustração da rede de peering de cluster

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

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



Informações relacionadas

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

["Considerações para configurar o peering de cluster"](#)

["Cabeamento das conexões de peering de cluster"](#)

["Peering dos clusters"](#)

Componentes de configuração de IP do MetroCluster necessários e convenções de nomenclatura

Identificar os componentes de hardware e software necessários e suportados para uma configuração IP MetroCluster . Analise as convenções de nomenclatura que os exemplos de documentação utilizam para os componentes.

Software e hardware suportados

O hardware e o software devem ser suportados para a configuração IP do MetroCluster.

["NetApp Hardware Universe"](#)

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

Requisitos de redundância de hardware em uma configuração IP MetroCluster

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

Requisitos de cluster do ONTAP em uma configuração IP do MetroCluster

As configurações IP do MetroCluster exigem dois clusters ONTAP, um em cada local do MetroCluster.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
- Local B: Cluster_B

Requisitos de switch IP em uma configuração IP MetroCluster

As configurações IP do MetroCluster requerem quatro switches IP. Os quatro switches formam duas malhas de armazenamento de switch que fornecem o ISL entre cada um dos clusters na configuração IP do MetroCluster.

Os switches IP também fornecem comunicação entre clusters entre os módulos do controlador em cada cluster.

A nomeação deve ser única dentro da configuração do MetroCluster.

Nomes de exemplo:

- Local A: Cluster_A
 - IP_switch_A_1
 - IP_switch_A_2
- Local B: Cluster_B
 - IP_switch_B_1
 - IP_switch_B_2

Requisitos do módulo do controlador em uma configuração IP do MetroCluster

As configurações IP do MetroCluster requerem quatro ou oito módulos de controlador.

Os módulos de controladora em cada local formam um par de HA. Cada módulo de controladora tem um parceiro de recuperação de desastres no outro local.

Cada módulo do controlador deve estar executando a mesma versão do ONTAP. Os modelos de plataforma compatíveis dependem da versão ONTAP:

- As novas instalações IP do MetroCluster em sistemas FAS não são suportadas no ONTAP 9.4.

As configurações de IP MetroCluster existentes em sistemas FAS podem ser atualizadas para ONTAP 9.4.

- A partir do ONTAP 9.5, são suportadas novas instalações MetroCluster IP em sistemas FAS.
- A partir do ONTAP 9.4, os módulos de controlador configurados para ADP são suportados.

Nomes de exemplo

Os seguintes nomes de exemplo são usados na documentação:

- Local A: Cluster_A
 - controller_A_1
 - controller_A_2
- Local B: Cluster_B
 - controller_B_1
 - controller_B_2

Requisitos de adaptador Gigabit Ethernet em uma configuração IP MetroCluster

As configurações IP do MetroCluster usam um adaptador Ethernet de 40/100 Gbps ou 10/25 Gbps para as interfaces IP para os switches IP usados para a malha IP do MetroCluster.



As portas integradas são incorporadas ao hardware do controlador (slot 0) e não podem ser substituídas, portanto, o slot necessário para o adaptador não é aplicável.

Modelo de plataforma	Adaptador Gigabit Ethernet necessário	Ranhura necessária para o adaptador	Portas
AFF A900, ASA A900 e FAS9500	X91146A	Slot 5, slot 7	e5b, e7b Observação: As portas e5a e e7a só podem ser usadas para LIFs intercluster. Você não pode usar essas portas para um LIF de dados.
AFF A700 e FAS9000	X91146A-C	Ranhura 5	e5a, e5b
AFF A800, AFF C800, ASA A800 e ASA C800	Portas de X1146A GbE/integradas	Slot 1/não aplicável para portas integradas	e0b, e1b
FAS8300, AFF A400, ASA A400, ASA C400, AFF C400	X1146A	Ranhura 1	e1a, e1b
AFF A300, FAS8200	X1116A	Ranhura 1	e1a, e1b
FAS2750, AFF A150, ASA A150, AFF A220	Portas integradas	Não aplicável	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250, AFF C250	Portas integradas	Não aplicável	e0c, e0d
AFF A320	Portas integradas	Não aplicável	e0g, e0h

AFF A70, FAS70, AFF C80	X50132A	Ranhura 2	e2a, e2b
AFF A90, AFF A1K, FAS90	X50132A	Slot 2, slot 3	e2b, e3b Observação: as portas E2A e E3A devem permanecer não utilizadas. O uso dessas portas para redes front-end ou peering não é suportado.
AFF A50	X60134A	Ranhura 2	e2a, e2b
AFF A30, AFF C30, AFF C60, FAS50	X60134A	Ranhura 2	e2a, e2b
AFF A20	X60132A	Slot 4, slot 2	e2b, e4b

"Saiba mais sobre atribuição automática de unidades e sistemas ADP em configurações IP do MetroCluster".

Requisitos de pool e unidade (mínimo suportado)

Uma configuração IP MetroCluster de quatro nós requer a configuração mínima em cada local:

- Cada nó tem pelo menos um pool local e um pool remoto no local.
- Pelo menos sete unidades em cada pool.

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



Os nomes dos agregados devem ser únicos em todos os sites MetroCluster. Isso significa que você não pode ter dois agregados diferentes com o mesmo nome no site A e no site B.

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

- Três unidades raiz
- Três unidades de dados
- Uma unidade sobressalente

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

As configurações do MetroCluster suportam RAID-DP, RAID4 e RAID-TEC.

 A partir do ONTAP 9.4, as configurações IP do MetroCluster suportam novas instalações usando atribuição automática de disco e ADP (particionamento avançado de unidade). "Considerações sobre atribuição automática de acionamento e sistemas ADP" Consulte para obter mais informações.

Considerações sobre o local da unidade para compartimentos parcialmente preenchidos

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

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

Considerações sobre o local da unidade para unidades internas AFF A800

Para a implementação correta do recurso ADP, os slots de disco do sistema AFF A800 devem ser divididos em trimestres e os discos devem ser localizados simetricamente nos trimestres.

Um sistema AFF A800 tem 48 compartimentos de unidade. As baías podem ser divididas em quartos:

- Quarto um:
 - Baías 0 - 5
 - Baías 24 - 29
- Quarto trimestre dois:
 - Baías 6 - 11
 - Baías 30 - 35
- Terceiro trimestre:
 - Baías 12 - 17
 - Baías 36 - 41
- Quarto trimestre:
 - Baías 18 - 23
 - Baías 42 - 47

Se este sistema estiver preenchido com 16 unidades, elas devem ser distribuídas simetricamente entre os quatro trimestres:

- Quatro unidades no primeiro trimestre: 0, 1, 2, 3
- Quatro unidades no segundo trimestre: 6, 7, 8, 9
- Quatro unidades no terceiro trimestre: 12, 13, 14, 15
- Quatro unidades no quarto trimestre: 18, 19, 20, 21

Componentes de hardware de configuração do MetroCluster IP

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

Sobre esta tarefa

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

Passos

1. Planeie o posicionamento dos componentes do MetroCluster.

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

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

Siga as etapas para *Instalar Hardware* nas instruções de *Instalação e Configuração* para o modelo da sua plataforma no "[Documentação dos sistemas de hardware ONTAP](#)" .

4. Instale os switches IP no rack ou gabinete.
5. Instale as gavetas de disco, ligue-as e, em seguida, defina as IDs das gaveta.

- É necessário desligar cada compartimento de disco.
- IDs de gaveta exclusivas são altamente recomendadas para cada gaveta de disco SAS em cada grupo de DR do MetroCluster para auxiliar na solução de problemas.



Não faça cabos com gavetas de disco destinadas a conter agregados sem espelhamento no momento. Você deve esperar para implantar gavetas destinadas a agregados sem espelhamento até que a configuração do MetroCluster esteja concluída e somente as implante depois de usar o `metrocluster modify -enable-unmirrored-aggr -deployment true` comando.

Cable os switches IP MetroCluster

Como usar as tabelas de portas com várias configurações de IP do MetroCluster

Você deve entender como usar as informações nas tabelas de portas para gerar corretamente seus arquivos RCF.

Antes de começar

Reveja estas considerações antes de utilizar as tabelas:

- As tabelas a seguir mostram o uso da porta para o local A. o mesmo cabeamento é usado para o local B.
- Não é possível configurar os switches com portas de velocidades diferentes (por exemplo, uma mistura de portas de 100 Gbps e portas de 40 Gbps).
- Mantenha o controle do grupo de portas MetroCluster (MetroCluster 1, MetroCluster 2, etc.). Você precisará dessas informações ao usar a ferramenta `RcfFileGenerator`, conforme descrito posteriormente neste procedimento de configuração.
- Você deve fazer o cabeamento de todos os nós da mesma maneira. Se houver diferentes opções de combinação de portas disponíveis para fazer o cabeamento dos nós, todos os nós devem usar as mesmas combinações de portas. Por exemplo, e1a em node1 e e1a em node2 devem ser conectados a um interruptor. Da mesma forma, a segunda porta de ambos os nós deve ser conectada ao segundo switch.
- O "[RcfFileGenerator para MetroCluster IP](#)" também fornece uma visão geral do cabeamento por porta para cada switch. Use esta visão geral do cabeamento para verificar o cabeamento.

Cabeamento de duas configurações MetroCluster para os switches

Ao conectar mais de uma configuração do MetroCluster a um switch, conecte cada MetroCluster de acordo com a tabela apropriada. Por exemplo, se você estiver conectando um FAS2750 e um AFF A700 ao mesmo switch, conecte o FAS2750 conforme "MetroCluster 1" na Tabela 1 e o AFF A700 conforme "MetroCluster 2" ou "MetroCluster 3" na Tabela 2. Não é possível ligar fisicamente o FAS2750 e o AFF A700 como "MetroCluster 1".

Cabeamento de configurações de MetroCluster de oito nós

Para a configuração do MetroCluster executando o ONTAP 9.8 e anterior, alguns procedimentos que são executados para fazer a transição de uma atualização exigem a adição de um segundo grupo de DR de quatro nós à configuração para criar uma configuração temporária de oito nós. A partir do ONTAP 9.9.1, são suportadas configurações permanentes de MetroCluster de oito nós.

Sobre esta tarefa

Para configurações de oito nós, use o mesmo método descrito acima. Em vez de um segundo MetroCluster, você está fazendo o cabeamento de um grupo adicional de DR de quatro nós.

Por exemplo, sua configuração inclui o seguinte:

- Interrutores Cisco 3132Q-V.
- MetroCluster 1: Plataformas FAS2750
- MetroCluster 2: Plataformas AFF A700 (essas plataformas estão sendo adicionadas como um segundo grupo de DR de quatro nós)

Passos

1. Para o MetroCluster 1, faça o cabeamento dos switches Cisco 3132Q-V usando a tabela para a plataforma FAS2750 e as linhas para interfaces MetroCluster 1.
2. Para o MetroCluster 2 (o segundo grupo DR), faça o cabeamento dos switches Cisco 3132Q-V usando a tabela para a plataforma AFF A700 e as linhas para interfaces MetroCluster 2.

Atribuições de portas de plataforma para switches Cisco 3132Q-V em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Reveja estas diretrizes antes de utilizar as tabelas:

- Se você configurar o switch para a transição MetroCluster FC para IP, a porta 5, a porta 6, a porta 13 ou a porta 14 podem ser usadas para conectar as interfaces de cluster locais do nó MetroCluster FC. Consulte "[RcfFileGenerator](#)" e os arquivos de cabeamento gerados para obter mais detalhes sobre o cabeamento dessa configuração. Para todas as outras conexões, você pode usar as atribuições de uso de portas listadas nas tabelas.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é...	Use esta tabela de cabeamento...
FAS2750, AFF A220	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 1)
FAS9000, AFF A700	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 2)
AFF A800, ASA A800	Atribuições de porta de plataforma Cisco 3132Q-V (grupo 3)

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 1)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS2750 ou AFF A220 para um switch Cisco 3132Q-V:

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8		ISL, Local Cluster	
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS9000 ou AFF A700 para um switch Cisco 3132Q-V:

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2		e4a	e4e / e8a
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4		e4a	e4e / e8a
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6		e4a	e4e / e8a
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10		e5a	e5b
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12		e5a	e5b
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14		e5a	e5b
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16		ISL, MetroCluster	
17		ISL, MetroCluster	
18		ISL, MetroCluster	
19		ISL, MetroCluster	
20		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4		ISL, MetroCluster	
23/1-4		ISL, MetroCluster	
24/1-4		ISL, MetroCluster	
25 - 32	Unused	disabled	

Atribuições de porta de plataforma Cisco 3132Q-V (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema AFF A800 ou ASA A800 para um switch Cisco 3132Q-V:

Switch Port	Port use	AFF A800 ASA A800		
		IP_Switch_x_1	IP_Switch_x_2	
1	MetroCluster 1, Local Cluster interface	e0a	e1a	
2				
3	MetroCluster 2, Local Cluster interface	e0a	e1a	
4				
5	MetroCluster 3, Local Cluster interface	e0a	e1a	
6				
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster		
8				
9	MetroCluster 1, MetroCluster interface	e0b	e1b	
10				
11	MetroCluster 2, MetroCluster interface	e0b	e1b	
12				
13	MetroCluster 3, MetroCluster interface	e0b	e1b	
14				
15	ISL, MetroCluster native speed 40G			
16				
17				
18		ISL, MetroCluster		
19				
20				
21/1-4	ISL, MetroCluster breakout mode 10G			
22/1-4				
23/1-4		ISL, MetroCluster		
24/1-4				
25 - 32	Unused	disabled		

Atribuições de porta de plataforma para switches Cisco 3232C ou Cisco 9336C de 36 portas em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Revise as seguintes considerações antes de usar as tabelas de configuração:

- As tabelas nesta seção são para switches Cisco 3232C ou switches Cisco 9336C-FX2 de 36 portas que não conectam armazenamento NS224.

Se você tiver um switch Cisco 9336C-FX2 de 12 portas, use as tabelas em "[Atribuições de portas de plataforma para switches Cisco 9336C-FX2 de 12 portas](#)" .

Se você tiver um switch Cisco 9336C-FX2 de 36 portas e pelo menos uma configuração MetroCluster ou grupo DR estiver conectando prateleiras NS224 ao switch MetroCluster, use as tabelas em "[Atribuições de porta de plataforma para um switch Cisco 9336C-FX2 de 36 portas conectando armazenamento NS224](#)" .

- As tabelas a seguir mostram o uso da porta para o local A. o mesmo cabeamento é usado para o local B.

- Não é possível configurar os switches com portas de velocidades diferentes (por exemplo, uma mistura de portas de 100 Gbps e portas de 40 Gbps).
- Se você estiver configurando um único MetroCluster com os switches, use o grupo de portas **MetroCluster 1**.

Mantenha o controle do grupo de portas MetroCluster (MetroCluster 1, MetroCluster 2, MetroCluster 3 ou MetroCluster 4). Você precisará dele ao usar a ferramenta RcfFileGenerator como descrito mais adiante neste procedimento de configuração.

- O RcfFileGenerator para MetroCluster IP também fornece uma visão geral de cabeamento por porta para cada switch.

Use esta visão geral do cabeamento para verificar o cabeamento.

- O arquivo RCF versão v2,10 ou posterior é necessário para o modo breakout 25G para ISLs MetroCluster.
- O ONTAP 9.13,1 ou posterior e o arquivo RCF versão 2,00 são necessários para usar uma plataforma diferente do FAS8200 ou do AFF A300 no grupo "MetroCluster 4".

 A versão do arquivo RCF é diferente da versão da ferramenta RCFfilegenerator usada para gerar o arquivo. Por exemplo, você pode gerar um arquivo RCF versão 2,00 usando o RCFfilegenerator v1,6c.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é...	Use esta tabela de cabeamento...
AFF A150, ASA A150 FAS2750, AFF A220 FAS500f, AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 1)
AFF A20	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 2)
AFF A30, AFF C30 FAS50 AFF C60	A tabela a seguir depende se você está usando uma placa Ethernet 25G (grupo 3a) ou 100g (grupo 3b). <ul style="list-style-type: none"> Atribuições de porta de plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 3a - 25G) Atribuições de porta de plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 3b - 100g)
FAS8200, AFF A300	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 4)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 5)
AFF A50	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 6)

Se o seu sistema é...	Use esta tabela de cabeamento...
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 7)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 8)

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 1)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	AFF A150		FAS500f	
		ASA A150	FAS2750	AFF A220	AFF C250
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 2)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A20 para um switch Cisco 3232C

ou 9336C-FX2:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e2a	e4a
5/2-4		disabled	
6/1		e2a	e4a
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e2b	e4b
13/2-4		disabled	
14/1		e2b	e4b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G		
16			
17			
18		ISL, MetroCluster	
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G		
22/1-4		ISL, MetroCluster	
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e2b	e4b
25/2-4		disabled	
26/1		e2b	e4b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e2a	e4a
29/2-4		disabled	
30/1		e2a	e4a
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Atribuições de porta de plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 3a)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 para um switch Cisco 3232C ou 9336C-FX2 usando uma placa Ethernet 25G de quatro portas.



Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5/1	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5/2-4		disabled		disabled		disabled	
6/1		e4a	e4b	e4a	e4b	e4a	e4b
6/2-4		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G						
8		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9		e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11		e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13		e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15							
16							
17		ISL, MetroCluster native speed 40G / 100G		ISL, MetroCluster		ISL, MetroCluster	
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G						
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28		Unused		disabled		disabled	
29/1		e4a	e4b	e4a	e4b	e4a	e4b
29/2-4	MetroCluster 4, Local Cluster interface	disabled		disabled		disabled	
30/1		e4a	e4b	e4a	e4b	e4a	e4b
30/2-4		disabled		disabled		disabled	
25 - 32		Unused		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)			disabled		disabled	

Atribuições de porta de plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 3b)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 para um switch Cisco 3232C ou 9336C-FX2 usando uma placa Ethernet 100g de duas portas.



Essa configuração requer uma placa ETHERNET 100g de duas portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
18		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
19	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
24/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
30		e4a	e4b	e4a	e4b	e4a	e4b
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 4)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS8200 ou AFF A300 para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
		e0a	e0b
1/1	MetroCluster 1, Local Cluster interface	disabled	
1/2-4		e0a	e0b
2/1		disabled	
2/2-4		e0a	e0b
3/1	MetroCluster 2, Local Cluster interface	disabled	
3/2-4		e0a	e0b
4/1		disabled	
4/2-4		e0a	e0b
5/1	MetroCluster 3, Local Cluster interface	disabled	
5/2-4		e0a	e0b
6/1		disabled	
6/2-4		e0a	e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8		e1a	e1b
9/1	MetroCluster 1, MetroCluster interface	disabled	
9/2-4		e1a	e1b
10/1		disabled	
10/2-4		e1a	e1b
11/1	MetroCluster 2, MetroCluster interface	disabled	
11/2-4		e1a	e1b
12/1		disabled	
12/2-4		e1a	e1b
13/1	MetroCluster 3, MetroCluster interface	disabled	
13/2-4		e1a	e1b
14/1		disabled	
14/2-4		e1a	e1b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16		ISL, MetroCluster	
17		ISL, MetroCluster	
18		ISL, MetroCluster	
19		ISL, MetroCluster	
20		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4		ISL, MetroCluster	
23/1-4		ISL, MetroCluster	
24/1-4		ISL, MetroCluster	
25/1	MetroCluster 4, MetroCluster interface	disabled	
25/2-4		e1a	e1b
26/1		disabled	
26/2-4		e1a	e1b
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	disabled	
29/2-4		e0a	e0b
30/1		disabled	
30/2-4		e0a	e0b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Se você estiver atualizando a partir de arquivos RCF mais antigos, a configuração de cabeamento pode estar usando portas no grupo "MetroCluster 4" (portas 25/26 e 29/30).

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 5)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A320, FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G						
16							
17		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G						
22/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	



O uso de portas no grupo "MetroCluster 4" requer o ONTAP 9.13,1 ou posterior.

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 6)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A50 para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6		e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b
14		e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16		ISL, MetroCluster	
17		ISL, MetroCluster	
18		ISL, MetroCluster	
19		ISL, MetroCluster	
20		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4		ISL, MetroCluster	
23/1-4		ISL, MetroCluster	
24/1-4		ISL, MetroCluster	
25	MetroCluster 4, MetroCluster interface	e2a	e2b
26		e2a	e2b
27 - 28	Unused	disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b
30		e4a	e4b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 7)

Revise as atribuições de portas da plataforma para enviar um sistema FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G						
16							
17		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
18							
19							
20	ISL, MetroCluster breakout mode 10G / 25G						
21/1-4							
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Nota 1: Utilize as portas e4a e e4e ou e4a e e8a se estiver a utilizar um adaptador X91440A (40Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).



O uso de portas no grupo "MetroCluster 4" requer o ONTAP 9.13.1 ou posterior.

Atribuições de porta da plataforma Cisco 3232C ou Cisco 9336C-FX2 (grupo 8)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K para um switch Cisco 3232C ou 9336C-FX2:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	ISL, Local Cluster native speed /100G	ISL, Local Cluster							
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15									
16									
17									
18									
19									
20									
21/1-4									
22/1-4									
23/1-4									
24/1-4									
25									
26	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
27 - 28	Unused	disabled		disabled		disabled		disabled	
29									
30	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
31 - 32	Unused	disabled		disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	

Atribuições de portas de plataforma para switches Cisco 9336C-FX2 de 12 portas em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Revise as seguintes considerações antes de usar as tabelas de configuração:

- As tabelas nesta seção são para switches Cisco 9336C-FX2 de 12 portas.

Se você tiver um switch Cisco 9336C-FX2 de 36 portas que não esteja conectando prateleiras NS224, use as tabelas em ["Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C-FX2 de 36 portas"](#).

Se você tiver um switch Cisco 9336C-FX2 de 36 portas e pelo menos uma configuração MetroCluster ou grupo DR estiver conectando prateleiras NS224 ao switch MetroCluster, use as tabelas em ["Atribuições de porta de plataforma para um switch Cisco 9336C-FX2 de 36 portas conectando armazenamento NS224"](#).



O switch Cisco 9336C-FX2 de 12 portas não suporta a conexão de prateleiras NS224 ao switch MetroCluster.

- As tabelas a seguir mostram o uso da porta para o local A. o mesmo cabeamento é usado para o local B.
- Não é possível configurar os switches com portas de velocidades diferentes (por exemplo, uma mistura de portas de 100 Gbps e portas de 40 Gbps).
- Se você estiver configurando um único MetroCluster com os switches, use o grupo de portas **MetroCluster 1**.

Monitore o grupo de portas do MetroCluster (MetroCluster 1, MetroCluster 2). Você precisará dele ao usar a ferramenta RcfFileGenerator, conforme descrito posteriormente neste procedimento de configuração.

- O RcfFileGenerator para MetroCluster IP também fornece uma visão geral de cabeamento por porta para cada switch.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é...	Use esta tabela de cabeamento...
AFF A150, ASAA150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 1)
AFF A20	Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 2)
AFF A30, AFF C30 FAS50 AFF C60	A tabela a seguir depende se você está usando uma placa Ethernet 25G (grupo 3a) ou 100g (grupo 3b). <ul style="list-style-type: none"> • Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 3a - 25G) • Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 3b - 100G)
FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 4)
AFF A50	Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 5)
AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Atribuições de portas da plataforma Cisco 9336C-FX2 de 12 portas (grupo 7)

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 1)

Revise as atribuições de porta da plataforma para cabear um sistema AFF A150, ASAA150, FAS500f, AFF C250, ASA C250, AFF A250 ou ASAA250 a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1-4	Unused	disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8		e0a	e0b	e0c	e0d
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	disabled		disabled	
9/2-4		e0a	e0b	e0c	e0d
10/1		disabled		disabled	
10/2-4		e0a	e0b	e0c	e0d
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Observação 1: Você só pode configurar as portas 19 e 20 ou as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 2)

Revise as atribuições de porta da plataforma para cabear um sistema AFF A20 a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1		e2a	e4a
1/2-4	MetroCluster 1, Local Cluster interface	disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1		e2a	e4a
3/2-4	MetroCluster 2, Local Cluster interface	disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8		e2b	e4b
9/1		disabled	
9/2-4	MetroCluster 1, MetroCluster interface	e2b	e4b
10/1		disabled	
10/2-4		e2b	e4b
11/1		disabled	
11/2-4	MetroCluster 2, MetroCluster interface	e2b	e4b
12/1		disabled	
12/2-4		e2b	e4b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked	

Observação 1: Você só pode configurar as portas 19 e 20 ou as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 3a)

Revise as atribuições de porta da plataforma para conectar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 a um switch Cisco 9336C-FX2 de 12 portas usando uma placa Ethernet 25G de quatro portas.



Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12	ISL, MetroCluster breakout mode 10G / 25G (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
13-18		blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked		blocked	

Observação 1: Você só pode configurar as portas 19 e 20 ou as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 3b)

Revise as atribuições de porta da plataforma para conectar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 a um switch Cisco 9336C-FX2 de 12 portas usando uma placa Ethernet 100G de duas portas.



Essa configuração requer uma placa ETHERNET 100g de duas portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked		blocked	

Observação 1: Você só pode configurar as portas 19 e 20 ou as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 4)

Revise as atribuições de porta da plataforma para cabear um sistema FAS8300, AFF C400, ASA C400, FAS8700, AFF A400 ou ASA A400 a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	FAS8300		AFF A400	
		AFF C400	ASA C400	ASA A400	FAS8700
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b
2					
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b
10					
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Observação 1: Você só pode configurar as portas 19 e 20 **ou** as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 5)

Revise as atribuições de porta da plataforma para cabear um sistema AFF A50 a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Observação 1: Você só pode configurar as portas 19 e 20 **ou** as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta da plataforma Cisco 9336C-FX2 de 12 portas (grupo 6)

Revise as atribuições de porta da plataforma para cabear um sistema AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900				
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2			
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)			
2								
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)			
4								
5-6	Ports disallowed to use		blocked		blocked			
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster			
8		ISL, Local Cluster			ISL, Local Cluster			
9	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b			
10								
11	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b			
12								
13-18	Ports disallowed to use		blocked		blocked			
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster			ISL, MetroCluster			
20		ISL, MetroCluster			ISL, MetroCluster			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster			ISL, MetroCluster			
22/1-4		ISL, MetroCluster			ISL, MetroCluster			
23-36	Ports disallowed to use		blocked		blocked			

Observação 1: Você só pode configurar as portas 19 e 20 **ou** as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Nota 2: Use as portas e4a e e4e ou e4a e e8a se estiver usando um adaptador X91440A (40 Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).

Atribuições de portas da plataforma Cisco 9336C-FX2 de 12 portas (grupo 7)

Revise as atribuições de porta da plataforma para cabear um sistema AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K a um switch Cisco 9336C-FX2 de 12 portas:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
8		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked		blocked		blocked	

Observação 1: Você só pode configurar as portas 19 e 20 **ou** as portas 21 e 22. Se você usar as portas 19 e 20 primeiro, as portas 21 e 22 serão bloqueadas. Se você usar as portas 21 e 22 primeiro, as portas 19 e 20 serão bloqueadas.

Atribuições de porta de plataforma para um switch Cisco 9336C-FX2 de 36 portas conectando armazenamento NS224 em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Revise as seguintes considerações antes de usar as tabelas de configuração:

- As tabelas nesta seção são para switches Cisco 9336C-FX2 de 36 portas quando pelo menos uma configuração MetroCluster ou grupo DR está conectando prateleiras NS224 ao switch MetroCluster.

Se você tiver um switch Cisco 9336C-FX2 de 36 portas e não planeja conectar o armazenamento NS224 ao switch, use as tabelas em "[Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C-FX2 de 36 portas](#)".

Se você tiver um switch Cisco 9336C-FX2 de 12 portas, use as tabelas em "[Atribuições de portas de plataforma para switches Cisco 9336C-FX2 de 12 portas](#)".



O switch Cisco 9336C-FX2 de 12 portas não suporta a conexão de prateleiras NS224 ao switch MetroCluster.

- Ao cabear um switch Cisco 9336C-FX2 conectando o armazenamento NS224, você pode ter no máximo duas configurações ou grupos de DR MetroCluster. Pelo menos uma configuração ou grupo de DR MetroCluster deve estar conectando os shelves NS224 ao switch MetroCluster. Se uma das suas configurações ou grupos de DR MetroCluster for um sistema que não suporta shelves NS224, ela só poderá ser conectada como a segunda configuração ou grupo de DR MetroCluster.

Se o seu segundo grupo MetroCluster ou DR não conectar as prateleiras NS224 ao switch MetroCluster, siga as instruções [tabelas de cabeamento para controladores que não conectam prateleiras NS224 conectadas a switches](#).

- O RcfFileGenerator só mostra as plataformas elegíveis quando a primeira plataforma é selecionada.
- A conexão de configurações de um MetroCluster de oito ou dois de quatro nós requer o ONTAP 9.14,1 ou posterior.

Escolha a tabela de cabeamento correta para sua configuração

Reveja a tabela de atribuições de portas correta para a sua configuração. Existem dois conjuntos de tabelas de cabeamento nesta seção:

- [Tabelas de cabeamento para controladores que conectam as gavetas NS224 conectadas ao switch](#)
- [Tabelas de cabeamento para controladores que não conectam as gavetas NS224 conectadas ao switch](#)

Controladores que conectam as NS224 gavetas conectadas ao switch

Determine a tabela de atribuições de portas que você deve seguir para os controladores que conectam as gavetas NS224 conectadas ao switch.

Plataforma	Use esta tabela de cabeamento...
AFF C30, AFF A30 AFF C60	A tabela a seguir depende se você está usando uma placa Ethernet 25G (grupo 1a) ou 100g (grupo 1b). <ul style="list-style-type: none"> • Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 1a - 25G) • Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 1b - 100g)
AFF A320 AFF C400, ASA C400 AFF A400, ASA A400	Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 2)
AFF A50	Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 3)
AFF A700 AFF C800, ASA C800, AFF A800 AFF A900, ASA A900	Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 4)
AFF A70 AFF C80 AFF A90 AFF A1K	Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 5)

Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 1a)

Revise as atribuições de portas da plataforma para fazer um cabo de um sistema AFF A30, AFF C30 ou AFF C60 que esteja conectando prateleiras NSS24 conectadas a switches a um switch Cisco 9336C-FX2 usando uma placa Ethernet 25G de quatro portas.



Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled	
2/1		e4a	e4b	e4a	e4b
2/2-4		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled	
4/1		e4a	e4b	e4a	e4b
4/2-4		disabled		disabled	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8		e2a	e2b	e2a	e2b
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14		ISL, MetroCluster		ISL, MetroCluster	
15		ISL, MetroCluster		ISL, MetroCluster	
16		ISL, MetroCluster		ISL, MetroCluster	
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18		e3a	e3b	e3a	e3b
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20		NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
21	Storage shelf 2 (8)	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
22					
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Switch Cisco 9336C-FX2 que conecta atribuições de portas de plataforma de storage NS224 (grupo 1b)

Revise as atribuições de portas da plataforma para fazer um cabo de um sistema AFF A30, AFF C30 ou AFF C60 que esteja conectando prateleiras NSS24 conectadas a switches a um switch Cisco 9336C-FX2 usando uma placa Ethernet 100g de duas portas.



Essa configuração requer uma placa ETHERNET 100g de duas portas no slot 4 para conectar o cluster local e as interfaces HA.

Controllers connecting switch-attached shelves						
Switch Port	Port Use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)		
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	
2		e4a	e4b	e4a	e4b	
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	
4		e4a	e4b	e4a	e4b	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	
7	ISL, Local Cluster native speed / 100G			ISL, Local Cluster		
8				ISL, Local Cluster		
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	
10		e2a	e2b	e2a	e2b	
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	
12		e2a	e2b	e2a	e2b	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G					
14				ISL, MetroCluster		
15				ISL, MetroCluster		
16						
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b	
18		e3a	e3b	e3a	e3b	
19	MetroCluster 2, Ethernet Storage Interface	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	
20		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	
21	Storage shelf 2 (8)					
22						
23	Storage shelf 3 (7)					
24						
25	Storage shelf 4 (6)					
26						
27	Storage shelf 5 (5)					
28						
29	Storage shelf 6 (4)					
30						
31	Storage shelf 7 (3)					
32						
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	

Switch Cisco 9336C-FX2 que conecta atribuições de portas da plataforma de storage NS224 (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A320, AFF C400, ASA C400, AFF A400 ou ASA A400 que esteja conectando gavetas NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
18							
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b				
28		NSM-2, e0a	NSM-2, e0b				
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Switch Cisco 9336C-FX2 que conecta atribuições de portas da plataforma de storage NS224 (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A50 que esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers connecting switch-attached shelves			
Switch Port	Port Use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8		ISL, Local Cluster	
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b
18			
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b
20			
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)		
28			
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b

Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 4)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A700, AFF C800, ASA C800, AFF A800, AFF A900 ou ASA A900 que esteja conectando as gavetas NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers connecting switch-attached shelves										
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900				
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2			
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1			
2										
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1			
4										
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
6										
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster				
8		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster				
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b			
10										
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b			
12										
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster				
14		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster				
15		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster				
16		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster				
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)			
18										
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)			
20										
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
22										
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
24										
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
26										
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
28										
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
30										
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
32										
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
34										
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b			
36										

Nota 1: Utilize as portas e4a e e4e ou e4a e e8a se estiver a utilizar um adaptador X91440A (40Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).

Switch Cisco 9336C-FX2 que coneta atribuições de portas de plataforma de storage NS224 (grupo 5)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A70, AFF C80, AFF A90 ou AFF A1K que esteja conectando gavetas NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers connecting switch-attached shelves									
Switch Port	Port Use	AFF A70		AFF C80		AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17	MetroCluster 1, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
18									
19	MetroCluster 2, Ethernet Storage Interface	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e11a (option 2) e8b (option 3)	e8b (option 1) e11b (option 2) e11a (option 3)	e8a (option 1) e9a (option 2) e10a (option 3) e11a (option 4) e8b (option 5) e10b (option 6)	e8b (option 1) e9b (option 2) e10b (option 3) e11b (option 4) e9a (option 5) e11a (option 6)
20									
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Controladores não conectando gavetas NS224 conectadas por switch

Determine a tabela de atribuições de portas que você deve seguir para os controladores que não estão conectando as gavetas NS224 conectadas a switch.

Plataforma	Use esta tabela de cabeamento...
AFF A150, ASA A150 FAS2750, AFF A220	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 6)
AFF A20	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 7)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 8)

Plataforma	Use esta tabela de cabeamento...
AFF C30, AFF A30 FAS50 AFF C60	A tabela a seguir depende se você está usando uma placa Ethernet 25G (grupo 9a) ou 100g (grupo 9b). <ul style="list-style-type: none"> O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 9a) O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 9b)
FAS8200, AFF A300	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 10)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 11)
AFF A50	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 12)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 13)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 14)

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 6)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A150, ASA A150, FAS2750 ou AFF A220 que não esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves				
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220		
		IP_Switch_x_1	IP_Switch_x_2	
1 - 6	Unused	disabled		
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		
8		ISL, Local Cluster		
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	
9/2-4		disabled		
10/1		e0a	e0b	
10/2-4		disabled		
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	
11/2-4		disabled		
12/1		e0a	e0b	
12/2-4		disabled		
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		
14		ISL, MetroCluster		
15		ISL, MetroCluster		
16		ISL, MetroCluster		
17-36	Unused	disabled		

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 7)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A20 que não esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8		ISL, Local Cluster	
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14		ISL, MetroCluster	
15		ISL, MetroCluster	
16		ISL, MetroCluster	
17-36	Unused	disabled	

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 8)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS500f, AFF C250, ASA C250, AFF A250 ou ASAA250 que não esteja conectando as gavetas NSS24 conectadas a switch a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves				
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250		
		IP_Switch_x_1	IP_Switch_x_2	
1 - 6	Unused	disabled		
7	ISL, Local Cluster native speed / 100G MetroCluster 1, Shared Cluster and MetroCluster interface	ISL, Local Cluster		
8		e0c	e0d	
9/1		disabled		
9/2-4		e0c	e0d	
10/1		disabled		
10/2-4		e0c	e0d	
11/1		e0c	e0d	
11/2-4		disabled		
12/1		e0c	e0d	
12/2-4		disabled		
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G			
14		ISL, MetroCluster		
15				
16				
17-36	Unused	disabled		

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 9a)

Revise as atribuições de portas da plataforma para realizar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 que não esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2 usando uma placa Ethernet 25G de quatro portas:



Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8		e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 9b)

Revise as atribuições de portas da plataforma para realizar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 que não esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2 usando uma placa Ethernet 100g de duas portas:



Essa configuração requer uma placa ETHERNET 100g de duas portas no slot 4 para conectar o cluster local e as interfaces HA.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3		e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8		e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 10)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS8200 ou AFF A300 que não esteja conectando as gavetas NSS24 conectadas a switch a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves				
Switch Port	Port Use	FAS8200		
		AFF A300		
		IP_Switch_x_1	IP_Switch_x_2	
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b	
1/2-4		disabled		
2/1		e0a	e0b	
2/2-4		disabled		
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b	
3/2-4		disabled		
4/1		e0a	e0b	
4/2-4		disabled		
5-6	Unused	disabled		
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		
8		e1a	e1b	
9/1	MetroCluster 1, MetroCluster interface	disabled		
9/2-4		e1a	e1b	
10/1		disabled		
10/2-4		e1a	e1b	
11/1	MetroCluster 2, MetroCluster interface	disabled		
11/2-4		e1a	e1b	
12/1		disabled		
12/2-4		e1a	e1b	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		
14		ISL, MetroCluster		
15		ISL, MetroCluster		
16		ISL, MetroCluster		
17-36	Unused	disabled		

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 11)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A320 ASA A400, FAS8700 Cisco, AFF C400 AFF A400 ou ASA C400 que não esteja conetando as gavetas NSS24 conetadas a um switch FAS8300 9336C-FX2:

Controllers not connecting switch-attached shelves						
Switch Port	Port Use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a
2						e3b
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a
4						e3b
5-6	Unused	disabled		disabled		disabled
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster
8						
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a
10						e1b
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a
12						e1b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster
14						
15						
16						
17-36	Unused	disabled		disabled		disabled

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 12)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A50 que não esteja conectando prateleiras NSS24 conectadas a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves						
Switch Port	Port use	AFF A50				
		IP_Switch_x_1	IP_Switch_x_2			
1	MetroCluster 1, Local Cluster interface	e4a	e4b			
2		e4a	e4b			
3	MetroCluster 2, Local Cluster interface	e4a	e4b			
4		e4a	e4b			
5-6	Unused	disabled				
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster				
8						
9	MetroCluster 1, MetroCluster interface	e2a	e2b			
10		e2a	e2b			
11	MetroCluster 2, MetroCluster interface	e2a	e2b			
12		e2a	e2b			
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster				
14						
15						
16						
17-36	Unused	disabled				

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 13)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS9000 Cisco, AFF A800 AFF A900, ASA A800 ASA A900, FAS9500, AFF A700 ou AFF C800 que não esteja conectando as gavetas NSS24 conectadas a um switch ASA C800 9336C-FX2:

Controllers not connecting switch-attached shelves							
Switch Port	Port Use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Nota 1: Utilize as portas e4a e e4e ou e4a e e8a se estiver a utilizar um adaptador X91440A (40Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).

O switch Cisco 9336C-FX2 não coneta atribuições de portas da plataforma de storage NS224 (grupo 14)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A70, FAS70, AFF C80, FAS90, AFF A90 ou AFF A1K que não esteja conetando as gavetas NSS24 conetadas a um switch Cisco 9336C-FX2:

Controllers not connecting switch-attached shelves									
Switch Port	Port Use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Unused	disabled		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster							
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14									
15									
16									
17-36	Unused	disabled		disabled		disabled		disabled	

Atribuições de porta de plataforma para switches IP BES-53248 com suporte da Broadcom em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Revise as seguintes considerações antes de usar as tabelas de configuração:

- Não é possível usar os switches com portas ISL remotas de diferentes velocidades (por exemplo, uma porta de 25 Gbps conectada a uma porta ISL de 10 Gbps).

- Se você configurar o switch para a transição MetroCluster FC para IP, as seguintes portas serão usadas dependendo da plataforma de destino escolhida:

Plataforma-alvo	Porta
Plataformas FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASAA400 ou FAS8700	Portas 1 - 6, 10Gbps
Plataformas FAS8200 ou AFF A300	Portas 3 - 4 e 9 - 12, 10Gbps

- Os sistemas AFF A320 configurados com switches BES-53248 Broadcom podem não suportar todos os recursos.

Qualquer configuração ou recurso que exija que as conexões do cluster local estejam conectadas a um switch não é suportado. Por exemplo, as seguintes configurações e procedimentos não são suportados:

- Configurações de MetroCluster de oito nós
- Transição das configurações MetroCluster FC para MetroCluster IP
- Atualizando uma configuração de IP MetroCluster de quatro nós (ONTAP 9.8 e posterior)

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é...	Use esta tabela de cabeamento...
AFF A150, ASAA150	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 1)
FAS2750	
AFF A220	
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 2)
AFF A20	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 3)
AFF C30, AFF A30 FAS50 AFF C60	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 4)
FAS8200, AFF A300	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 5)
AFF A320	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 6)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Atribuições de porta de plataforma Broadcom BES-53248 (grupo 7)

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 1)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A150, ASAA150, FAS2750 ou AFF A220 para um switch BES-53248 da Broadcom:

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused		disabled
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Nota 1:** O uso dessas portas requer uma licença adicional.
- Se ambas as configurações do MetroCluster estiverem usando a mesma plataforma, a NetApp recomenda selecionar o grupo "MetroCluster 3" para uma configuração e o grupo "MetroCluster 4" para a outra configuração. Se as plataformas forem diferentes, você deve selecionar "MetroCluster 3" ou "MetroCluster 4" para a primeira configuração e "MetroCluster 1" ou "MetroCluster 2" para a segunda configuração.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 2)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	ISL, MetroCluster
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	ISL, Local Cluster
56			

- **Nota 1:** O uso dessas portas requer uma licença adicional.
- Se ambas as configurações do MetroCluster estiverem usando a mesma plataforma, a NetApp recomenda selecionar o grupo "MetroCluster 3" para uma configuração e o grupo "MetroCluster 4" para a outra configuração. Se as plataformas forem diferentes, você deve selecionar "MetroCluster 3" ou "MetroCluster 4" para a primeira configuração e "MetroCluster 1" ou "MetroCluster 2" para a segunda configuração.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 3)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema AFF A20 para um switch BES-53248 Broadcom:

Physical Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e2a	e4a
2			
3	MetroCluster 2, Local Cluster interface	e2a	e4a
4			
5	MetroCluster 1, MetroCluster interface	e2b	e4b
6			
7	MetroCluster 2, MetroCluster interface	e2b	e4b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 3, Local Cluster interface (note 1)	e2a	e4a
18			
19	MetroCluster 3, MetroCluster interface (note 1)	e2b	e4b
20			
21	MetroCluster 4, Local Cluster interface (note 1)	e2a	e4a
22			
23	MetroCluster 4, MetroCluster interface (note 1)	e2b	e4b
24			
..	Ports not licensed (25 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Nota 1:** O uso dessas portas requer uma licença adicional.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 4)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema AFF A30, AFF C30, AFF C60 ou FAS50 para um switch BES-53248 Broadcom usando uma placa Ethernet 25G de quatro portas.

- Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.
- Esta configuração requer um adaptador QSFP-to-SFP na placa do controlador para suportar uma velocidade de rede de 25GbpsMbps.

Physical Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4							
5	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
6							
7	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9 - 12	Unused	disabled		disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster
14							
15							
16							
17	MetroCluster 3, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
18							
19	MetroCluster 3, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
20							
21	MetroCluster 4, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
22							
23	MetroCluster 4, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
24							
..	Ports not licensed (25 - 54)						
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster
54							
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	ISL, Local Cluster	ISL, Local Cluster	ISL, Local Cluster	ISL, Local Cluster	ISL, Local Cluster
56							

- **Nota 1:** O uso dessas portas requer uma licença adicional.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 5)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema FAS8200 ou AFF A300 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7			
8	MetroCluster 2, MetroCluster interface	e1a	e1b
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	ISL, MetroCluster
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	ISL, MetroCluster
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	ISL, Local Cluster
56			

- **Nota 1:** O uso dessas portas requer uma licença adicional.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 6)

Revise as atribuições de portas da plataforma para fazer o cabo de um sistema AFF A320 para um switch BES-53248 Broadcom:

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
55			
56			

- **Nota 1:** O uso dessas portas requer uma licença adicional.

- **Nota 2:** Apenas um único MetroCluster de quatro nós usando sistemas AFF A320 pode ser conectado ao switch.

Os recursos que exigem um cluster comutado não são suportados nesta configuração. Isso inclui os procedimentos de transição FC para IP do MetroCluster e atualização técnica.

Atribuições de porta de plataforma Broadcom BES-53248 (grupo 7)

Revise as atribuições de portas da plataforma para fazer o cabeamento de um sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 ou FAS8700 para um switch BES-53248 da Broadcom:

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1 - 12	Ports not used (see Note 2)	disabled		disabled		
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster		
14						
15						
16						
..	Ports not licensed (17 - 48)					
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b	
50	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b	
51						
52	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	ISL, MetroCluster	ISL, MetroCluster		
53						
54						
55						
56	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		

- **Nota 1:** O uso dessas portas requer uma licença adicional.
- **Nota 2:** Apenas um único MetroCluster de quatro nós usando sistemas AFF A320 pode ser conectado ao switch.

Os recursos que exigem um cluster comutado não são suportados nesta configuração. Isso inclui os procedimentos de transição FC para IP do MetroCluster e atualização técnica.

Atribuições de porta de plataforma para switches IP SN2100 com suporte da NVIDIA em uma configuração IP MetroCluster

O uso da porta em uma configuração IP do MetroCluster depende do modelo do switch e do tipo de plataforma.

Revise as seguintes considerações antes de usar as tabelas de configuração:

- A conexão de configurações de MetroCluster de oito ou dois nós requer o ONTAP 9.14,1 ou posterior e o arquivo RCF versão 2,00 ou posterior.



A versão do arquivo RCF é diferente da versão da ferramenta RCFfilegenerator usada para gerar o arquivo. Por exemplo, você pode gerar um arquivo RCF versão 2,00 usando o RCFfilegenerator v1,6c.

- Se você fizer o cabo de várias configurações do MetroCluster, siga a respetiva tabela. Por exemplo:
 - Se você fizer o cabo de duas configurações MetroCluster de quatro nós do tipo AFF A700, conecte o primeiro MetroCluster mostrado como "MetroCluster 1" e o segundo MetroCluster mostrado como "MetroCluster 2" na tabela AFF A700.



As portas 13 e 14 podem ser usadas no modo de velocidade nativo que suporta 40 Gbps e 100 Gbps, ou no modo de breakout para suportar 4 x 25 Gbps ou 4 x 10 Gbps. Se eles usam o modo de velocidade nativa, eles são representados como portas 13 e 14. Se eles usam o modo breakout, 4 x 25 Gbps ou 4 x 10 Gbps, então eles são representados como portas 13s0-3 e 14s0-3.

As seções a seguir descrevem o contorno físico do cabeamento. Você também pode consultar o "[RcfFileGenerator](#)" para obter informações detalhadas sobre cabeamento.

Escolha a tabela de cabeamento correta para sua configuração

Use a tabela a seguir para determinar qual tabela de cabeamento você deve seguir.

Se o seu sistema é...	Use esta tabela de cabeamento...
AFF A150, ASA A150	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 1)
FAS500f	
AFF C250, ASA C250	
AFF A250, ASA A250	
AFF A20	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 2)

Se o seu sistema é...	Use esta tabela de cabeamento...
AFF C30, AFF A30 FAS50 AFF C60	A tabela a seguir depende se você está usando uma placa Ethernet 25G (grupo 3a) ou 100g (grupo 3b). <ul style="list-style-type: none"> Atribuições de porta da plataforma NVIDIA SN2100 (grupo 3a -25G) Atribuições de porta da plataforma NVIDIA SN2100 (grupo 3b -100g)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700 FAS9000, AFF A700	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 4)
AFF A50	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 5)
AFF C800, ASA C800 AFF A800, ASA A800 FAS9500 AFF A900, ASA A900	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Atribuições de portas da plataforma NVIDIA SN2100 (grupo 7)

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 1)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 ou ASA A250 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, Local Cluster 100G		ISL, Local Cluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16		ISL, Local Cluster		ISL, Local Cluster	

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 2)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A20 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF A20		
		IP_Switch_x_1	IP_Switch_x_2	
1s0	MetroCluster 1, Local Cluster interface	e2a	e4a	
s1s1-3		disabled		
2s0		e2a	e4a	
2s1-3		disabled		
3s0	MetroCluster 2, Local Cluster interface	e2a	e4a	
3s1-3		disabled		
4s0		e2a	e4a	
4s1-3		disabled		
5s0	MetroCluster 3, Local Cluster interface	e2a	e4a	
5s1-3		disabled		
6s0		e2a	e4a	
6s1-3		disabled		
7	MetroCluster 1, MetroCluster interface	e2b	e4b	
8				
9				
10	MetroCluster 2, MetroCluster interface	e2b	e4b	
11				
12				
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		
14 / 14s0-3		ISL, MetroCluster		
15	ISL, Local Cluster 100G	ISL, Local Cluster		
16		ISL, Local Cluster		

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 3a)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 para um switch NVIDIA SN2100 usando uma placa Ethernet 25G de quatro portas:



Essa configuração requer uma placa Ethernet 25G de quatro portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8		e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, Local Cluster 100G		ISL, Local Cluster		ISL, Local Cluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 3b)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A30, AFF C30, AFF C60 ou FAS50 para um switch NVIDIA SN2100 usando uma placa Ethernet 100g de duas portas:



Essa configuração requer uma placa ETHERNET 100g de duas portas no slot 4 para conectar o cluster local e as interfaces HA.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8		e2a	e2b	e2a	e2b	e2a	e2b
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, Local Cluster 100G		ISL, Local Cluster		ISL, Local Cluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 4)

Revise as atribuições de portas da plataforma para enviar um sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000 ou AFF A700 para um switch NVIDIA SN2100:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700			AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1	
2								
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1	
4								
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a Note 1	
6								
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	
8								
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	
10								
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	
12								
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G			ISL, MetroCluster		ISL, MetroCluster		
14 / 14s0-3						ISL, MetroCluster		
15	ISL, Local Cluster 100G			ISL, Local Cluster		ISL, Local Cluster		
16						ISL, Local Cluster		

Nota 1: Utilize as portas e4a e e4e ou e4a e e8a se estiver a utilizar um adaptador X91440A (40Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 5)

Revise as atribuições de portas da plataforma para enviar um sistema AFF A50 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6			
7	MetroCluster 1, MetroCluster interface	e2a	e2b
8			
9	MetroCluster 2, MetroCluster interface	e2a	e2b
10			
11	MetroCluster 3, MetroCluster interface	e2a	e2b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G		
14 / 14s0-3		ISL, MetroCluster	
15	ISL, Local Cluster 100G		
16		ISL, Local Cluster	

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 6)

Revise as atribuições de portas da plataforma para enviar um sistema AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 ou ASA A900 para um switch NVIDIA SN2100:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Nota 1: Utilize as portas e4a e e4e ou e4a e e8a se estiver a utilizar um adaptador X91440A (40Gbps). Utilize as portas e4a e e4b ou e4a e e8a se estiver a utilizar um adaptador X91153A (100Gbps).

Atribuições de portas da plataforma NVIDIA SN2100 (grupo 7)

Reveja as atribuições de portas da plataforma para o cabo de um sistema FAS70, AFF A70, AFF C80, FAS90, AFF A90 ou AFF A1K para um switch NVIDIA SN2100:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
8									
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
12									
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3									
15	ISL, Local Cluster 100G	ISL, Local Cluster							
16									

Cabear as portas do módulo controlador ONTAP em uma configuração IP do MetroCluster

Você deve fazer o cabeamento das portas do módulo do controlador usadas para peering de cluster, gerenciamento e conetividade de dados.

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

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

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

- Identifique e faça a cabeamento de pelo menos duas portas para peering de cluster e verifique se elas têm

conetividade de rede com o cluster do parceiro.

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

"Configuração expressa de peering de cluster e SVM"

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

Use as instruções de instalação da sua plataforma no "["Documentação dos sistemas de hardware da ONTAP"](#)".



Os sistemas IP da MetroCluster não têm portas de alta disponibilidade (HA) dedicadas. Dependendo da sua plataforma, o tráfego de HA é servido usando o MetroCluster, o cluster local ou a interface de cluster/MetroCluster compartilhado. Ao usar *Documentação de sistemas de hardware ONTAP* para instalar sua plataforma, você não deve seguir as instruções para fazer o cabeamento do cluster e das portas HA.

Configure os switches IP MetroCluster

Escolha o procedimento correto de configuração do switch IP do MetroCluster

Você deve configurar os switches IP para fornecer conetividade IP do MetroCluster de back-end. O procedimento a seguir depende do fornecedor do seu switch.

- ["Configurar switches IP Broadcom"](#)
- ["Configurar switches IP Cisco"](#)
- ["Configurar switches IP NVIDIA"](#)

Configurar switches IP Broadcom para interconexão de cluster e conectividade IP MetroCluster de backend

Você deve configurar os switches IP Broadcom para uso como interconexão de cluster e para conetividade IP MetroCluster de back-end.



A sua configuração requer licenças adicionais (6 licença de porta de 100 GB) nos seguintes cenários:

- Você usa as portas 53 e 54 como um ISL MetroCluster de 40 Gbps ou 100 Gbps.
- Você usa uma plataforma que conecta o cluster local e as interfaces MetroCluster às portas 49 - 52.

Redefinindo o switch IP Broadcom para os padrões de fábrica

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

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.

- Você deve estar conectado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Mude para o prompt de comando elevado (#): enable

```
(IP_switch_A_1)> enable  
(IP_switch_A_1) #
```

2. Apague a configuração de inicialização e remova o banner

- a. Apagar a configuração de arranque:

```
erase startup-config
```

```
(IP_switch_A_1) #erase startup-config  
  
Are you sure you want to clear the configuration? (y/n) y  
  
(IP_switch_A_1) #
```

Este comando não apaga o banner.

- b. Remova o banner:

```
no set clibanner
```

```
(IP_switch_A_1) #configure  
(IP_switch_A_1) (Config) # no set clibanner  
(IP_switch_A_1) (Config) #
```

3. Reinicie o switch: **(IP_switch_A_1) #reload**

```
Are you sure you would like to reset the system? (y/n) y
```



Se o sistema perguntar se deseja salvar a configuração não salva ou alterada antes de recarregar o switch, selecione **não**.

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

O usuário padrão é "admin", e nenhuma senha é definida. É apresentado um aviso semelhante ao seguinte:

```
(Routing) >
```

5. Mude para o prompt de comando elevado:

```
enable
```

```
Routing) > enable  
(Routing) #
```

6. Defina o protocolo da porta de serviço como none:

```
serviceport protocol none
```

```
(Routing) #serviceport protocol none  
Changing protocol mode will reset ip configuration.  
Are you sure you want to continue? (y/n) y  
(Routing) #
```

7. Atribua o endereço IP à porta de serviço:

```
serviceport ip ip-address netmask gateway
```

O exemplo a seguir mostra um endereço IP atribuído à porta de serviço "10.10.10.10" com a sub-rede "255.255.255.0" e o gateway "10.10.10.1":

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Verifique se a porta de serviço está configurada corretamente:

```
show serviceport
```

O exemplo a seguir mostra que a porta está ativa e os endereços corretos foram atribuídos:

```
(Routing) #show serviceport

Interface Status..... Up
IP Address..... 10.10.10.10
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.10.10.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router..... fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol..... None
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Burned In MAC Address..... D8:C4:97:56:87:D7

(Routing) #
```

9. Configure o servidor SSH.



- O arquivo RCF desativa o protocolo Telnet. Se você não configurar o servidor SSH, você só poderá acessar a ponte usando a conexão de porta serial.
- Você deve configurar o servidor SSH para usar a coleta de logs e outras ferramentas externas.

a. Gerar chaves RSA.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. Gerar chaves DSA (opcional)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Se você estiver usando a versão compatível com FIPS do EFOS, gere as chaves ECDSA. O exemplo a seguir cria as teclas com um comprimento de 521. Os valores válidos são 256, 384 ou 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Ative o servidor SSH.

Se necessário, saia do contexto de configuração.

```
(Routing) (Config) #end  
(Routing) #ip ssh server enable
```

+



Se as chaves já existem, então você pode ser solicitado a sobrescrevê-las.

10. Se desejar, configure o domínio e o servidor de nomes:

configure

O exemplo a seguir mostra ip domain os comandos e ip name server:

```
(Routing) # configure  
(Routing) (Config) #ip domain name lab.netapp.com  
(Routing) (Config) #ip name server 10.99.99.1 10.99.99.2  
(Routing) (Config) #exit  
(Routing) (Config) #
```

11. Se desejar, configure o fuso horário e a sincronização de horário (SNTP).

O exemplo a seguir mostra os sntp comandos, especificando o endereço IP do servidor SNTP e o fuso horário relativo.

```
(Routing) #  
(Routing) (Config) #sntp client mode unicast  
(Routing) (Config) #sntp server 10.99.99.5  
(Routing) (Config) #clock timezone -7  
(Routing) (Config) #exit  
(Routing) (Config) #
```

Para o EFOS versão 3.10.0.3 e posterior, use o ntp comando, como mostrado no exemplo a seguir:

```

> (Config) # ntp ?

authenticate          Enables NTP authentication.
authentication-key    Configure NTP authentication key.
broadcast             Enables NTP broadcast mode.
broadcastdelay        Configure NTP broadcast delay in microseconds.
server                Configure NTP server.
source-interface      Configure the NTP source-interface.
trusted-key           Configure NTP authentication key number for
trusted time source.
vrf                  Configure the NTP VRF.

>(Config) # ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config) # ntp server 10.99.99.5

```

12. Configure o nome do switch:

```
hostname IP_switch_A_1
```

O prompt do switch exibirá o novo nome:

```

(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #

```

13. Guardar a configuração:

```
write memory
```

Você recebe prompts e saída semelhantes ao seguinte exemplo:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!

(IP_switch_A_1) #
```

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

Download e instalação do software Broadcom switch EFOS

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa deve ser repetida em cada switch na configuração IP do MetroCluster.

Observe o seguinte:

- Ao atualizar do EFOS 3,4.x.x para o EFOS 3,7.x.x ou posterior, o switch deve estar executando o EFOS 3.4.4.6 (ou versão 3,4.x.x posterior). Se você estiver executando uma versão antes disso, atualize o switch para EFOS 3.4.4.6 (ou versão posterior 3,4.x.x) primeiro, então atualize o switch para EFOS 3,7.x.x ou posterior.
- A configuração para o EFOS 3,4.x.x e 3,7.x.x ou posterior é diferente. Alterar a versão do EFOS de 3,4.x.x para 3,7.x.x ou posterior, ou vice-versa, requer que o switch seja redefinido para os padrões de fábrica e os arquivos RCF para que a versão do EFOS correspondente seja (re)aplicada. Este procedimento requer acesso através da porta do console serial.
- A partir da versão 3,7.x.x do EFOS ou posterior, uma versão não compatível com FIPS e compatível com FIPS está disponível. Diferentes etapas se aplicam ao passar de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa. Alterar o EFOS de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa redefinirá o switch para os padrões de fábrica. Este procedimento requer acesso através da porta do console serial.

Passos

1. Transfira o firmware do switch a partir do "[Site de suporte da Broadcom](#)".
2. Verifique se sua versão do EFOS é compatível com FIPS ou não compatível com FIPS usando o `show fips status` comando. Nos exemplos a seguir `IP_switch_A_1`, está usando EFOS compatível com FIPS e `IP_switch_A_2` está usando EFOS não compatível com FIPS.

Exemplo 1

```

IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #

```

Exemplo 2

```

IP_switch_A_2 #show fips status
^
% Invalid input detected at `^` marker.

IP_switch_A_2 #

```

3. Use a tabela a seguir para determinar qual método você deve seguir:

Procedimento	Versão atual do EFOS	Nova versão EFOS	Passos de alto nível
Etapas para atualizar o EFOS entre duas versões (não) compatíveis com FIPS	3.4.x.x	3.4.x.x	Instale a nova imagem EFOS utilizando o método 1) as informações de configuração e licença são mantidas
3.4.4.6 (ou posterior 3.4.x.x)	3.7.x.x ou posterior não compatível com FIPS	Atualize o EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3.7.x.x ou posterior	3.7.x.x ou posterior não compatível com FIPS
3.4.4.6 (ou posterior 3.4.x.x)	Downgrade EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3.4.x.x	3.7.x.x ou posterior não compatível com FIPS	
Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas	3.7.x.x ou posterior compatível com FIPS	3.7.x.x ou posterior compatível com FIPS	Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas

Passos para atualizar para/a partir de uma versão EFOS compatível com FIPS	Não compatível com FIPS	Compatível com FIPS	Instalação da imagem EFOS usando o método 2. A configuração do switch e as informações da licença serão perdidas.
--	-------------------------	---------------------	---

- Método 1: [Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup](#)
- Método 2: [Etapas para atualizar o EFOS usando a instalação do ONIE os](#)

Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup

Só pode executar as seguintes etapas se ambas as versões do EFOS forem não compatíveis com FIPS ou ambas as versões do EFOS forem compatíveis com FIPS.



Não utilize estes passos se uma versão for compatível com FIPS e a outra não for compatível com FIPS.

Passos

1. Copie o software do interruptor para o interruptor: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

Neste exemplo, o arquivo do sistema operacional `efos-3.4.4.6.stk` é copiado do servidor SFTP em `50.50.50.50` para a partição de backup. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-  
3.4.4.6.stk backup  
Remote Password:*****  
  
Mode..... SFTP  
Set Server IP..... 50.50.50.50  
Path..... /switchsoftware/  
Filename..... efos-3.4.4.6.stk  
Data Type..... Code  
Destination Filename..... backup  
  
Management access will be blocked for the duration of the transfer  
Are you sure you want to start? (y/n) y  
  
File transfer in progress. Management access will be blocked for the  
duration of the transfer. Please wait...  
SFTP Code transfer starting...  
  
File transfer operation completed successfully.  
  
(IP_switch_A_1) #
```

2. Configure o switch para inicializar a partir da partição de backup na próxima reinicialização do switch:

```
boot system backup
```

```
(IP_switch_A_1) #boot system backup  
Activating image backup ..  
  
(IP_switch_A_1) #
```

3. Verifique se a nova imagem de inicialização estará ativa na próxima inicialização:

```
show bootvar
```

```
(IP_switch_A_1) #show bootvar
```

Image Descriptions

```
active :  
backup :
```

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.4.2	3.4.4.6	3.4.4.2	3.4.4.6

```
(IP_switch_A_1) #
```

4. Guardar a configuração:

```
write memory
```

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!

```
(IP_switch_A_1) #
```

5. Reinicie o switch:

```
reload
```

```
(IP_switch_A_1) #reload
```

Are you sure you would like to reset the system? (y/n) y

6. Aguarde até que o switch seja reiniciado.



Em cenários raros, o switch pode falhar ao inicializar. Siga o [Etapas para atualizar o EFOS usando a instalação do ONIE os](#) para instalar a nova imagem.

7. Se alterar a mudança de EFOS 3,4.x.x para EFOS 3,7.x.x ou vice-versa, siga os dois procedimentos a seguir para aplicar a configuração correta (RCF):
 - a. [Redefinindo o switch IP Broadcom para os padrões de fábrica](#)
 - b. [Download e instalação dos arquivos RCF Broadcom](#)
8. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Etapas para atualizar o EFOS usando a instalação do ONIE os

Pode executar as seguintes etapas se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS. Estas etapas podem ser usadas para instalar a imagem EFOS 3,7.x.x não compatível com FIPS do ONIE se o switch não inicializar.

Passos

1. Inicialize o switch no modo de instalação ONIE.

Durante a inicialização, selecione ONIE quando a seguinte tela for exibida:

```
+-----+  
| EFOS |  
| *ONIE |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
|       |  
+-----+
```

Depois de selecionar "ONIE", o switch irá então carregar e apresentar-lhe as seguintes opções:

```
+-----+  
| *ONIE: Install OS  
| ONIE: Rescue  
| ONIE: Uninstall OS  
| ONIE: Update ONIE  
| ONIE: Embed ONIE  
| DIAG: Diagnostic Mode  
| DIAG: Burn-In Mode  
|  
|  
|  
|  
|  
|  
+-----+
```

O switch agora será inicializado no modo de instalação ONIE.

2. Pare a descoberta ONIE e configure a interface ethernet

Quando a seguinte mensagem for exibida, pressione <enter> para chamar o console ONIE:

```
Please press Enter to activate this console. Info: eth0: Checking  
link... up.  
ONIE:/ #
```



A descoberta ONIE continuará e as mensagens serão impressas no console.

```
Stop the ONIE discovery  
ONIE:/ # onie-discovery-stop  
discover: installer mode detected.  
Stopping: discover... done.  
ONIE:/ #
```

3. Configure a interface ethernet e adicione a rota utilizando ifconfig eth0 <ipAddress> netmask <netmask> up e route add default gw <gatewayAddress>

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up  
ONIE:/ # route add default gw 10.10.10.1
```

4. Verifique se o servidor que hospeda o arquivo de instalação ONIE está acessível:

```

ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #

```

5. Instale o novo software do interruptor

```

ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.

```

O software irá instalar e, em seguida, reiniciar o interruptor. Deixe o switch reiniciar normalmente para a nova versão do EFOS.

6. Verifique se o novo software do switch está instalado

show bootvar

```

(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
-----
unit    active    backup    current-active   next-active
-----
1      3.7.0.4     3.7.0.4   3.7.0.4           3.7.0.4
(Routing) #

```

7. Conclua a instalação

O switch reiniciará sem nenhuma configuração aplicada e redefinirá os padrões de fábrica. Siga os dois procedimentos para configurar as configurações básicas do switch e aplicar o arquivo RCF conforme descrito nos dois documentos a seguir:

- a. Configure as definições básicas do interruptor. Siga o passo 4 e posterior: [Redefinindo o switch IP Broadcom para os padrões de fábrica](#)
- b. Crie e aplique o arquivo RCF conforme descrito em [Download e instalação dos arquivos RCF Broadcom](#)

Download e instalação dos arquivos RCF Broadcom

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

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

Sobre esta tarefa

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

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

Interrutor	Ficheiro RCF
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt



Os arquivos RCF para EFOS versão 3.4.4.6 ou posterior versão 3.4.x.x. e EFOS versão 3.7.0.4 são diferentes. Você precisa ter certeza de que criou os arquivos RCF corretos para a versão EFOS em que o switch está sendo executado.

Versão de EFOS	Versão do ficheiro RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Passos

1. Gere os arquivos RCF Broadcom para MetroCluster IP.
 - a. Transfira o. ["RcfFileGenerator para MetroCluster IP"](#)
 - b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.



As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:

- a. Copie os arquivos RCF para o primeiro switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

Neste exemplo, o arquivo RCF "BES-53248_v1.32_Switch-A1.txt" é copiado do servidor SFTP em "50.50.50.50" para o flash de inicialização local. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-  
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr
```

```
Remote Password:*****
```

```
Mode..... SFTP  
Set Server IP..... 50.50.50.50  
Path..... /RcfFiles/  
Filename..... BES-  
53248_v1.32_Switch-A1.txt  
Data Type..... Config Script  
Destination Filename..... BES-  
53248_v1.32_Switch-A1.scr
```

```
Management access will be blocked for the duration of the transfer  
Are you sure you want to start? (y/n) y
```

```
File transfer in progress. Management access will be blocked for the  
duration of the transfer. Please wait...  
File transfer operation completed successfully.
```

```
Validating configuration script...
```

```
config
```

```
set clibanner
```

```
"*****
```

```
*****
```

```
* NetApp Reference Configuration File (RCF)
```

```
*
```

```
* Switch      : BES-53248
```

```
...
```

```
The downloaded RCF is validated. Some output is being logged here.
```

```
...
```

```
Configuration script validated.
```

```
File transfer operation completed successfully.
```

```
(IP_switch_A_1) #
```

b. Verifique se o arquivo RCF está salvo como um script:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name          Size(Bytes) Date of Modification
-----
BES-53248_v1.32_Switch-A1.scr      852       2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Aplicar o script RCF:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y

config

set clibanner
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : BES-53248
...
The downloaded RCF is validated. Some output is being logged here.
...
Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Guardar a configuração:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!

(IP_switch_A_1) #
```

e. Reinicie o switch:

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

- a. Repita os passos anteriores para cada uma das outras três centrais, certificando-se de copiar o ficheiro RCF correspondente para o comutador correspondente.

3. Recarregue o interruptor:

```
reload
```

```
IP_switch_A_1# reload
```

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

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:



Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

Para detalhes da porta ISL

Executar o comando `show port all`.

Para obter detalhes do canal da porta

Executar o comando `show port-channel all`.

2. Desative as portas ISL e os canais de portas não utilizados.

Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
(SwtichA_1)> enable  
(SwtichA_1)# configure  
(SwtichA_1) (Config)# <port_name>  
(SwtichA_1) (Interface 0/15)# shutdown  
(SwtichA_1) (Interface 0/15)# end  
(SwtichA_1)# write memory
```

Configurar switches IP Cisco

Configurar switches IP da Cisco para interconexão de cluster e conectividade IP MetroCluster de backend

Você deve configurar os switches IP Cisco para uso como interconexão de cluster e para conectividade IP do MetroCluster de back-end.

Sobre esta tarefa

Vários dos procedimentos nesta seção são procedimentos independentes e você só precisa executar aqueles para os quais você é direcionado ou é relevante para a sua tarefa.

Rapor as predefinições de fábrica do interruptor IP do Cisco

Antes de instalar qualquer arquivo RCF, você deve apagar a configuração do switch Cisco e executar a configuração básica. Este procedimento é necessário quando você deseja reinstalar o mesmo arquivo RCF depois de uma instalação anterior falhar, ou se você quiser instalar uma nova versão de um arquivo RCF.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conectado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Repor as predefinições de fábrica do interruptor:

- a. Apagar a configuração existente:

```
write erase
```

b. Recarregue o software do switch:

```
reload
```

O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt "Cancelar provisionamento automático e continuar com a configuração normal? (sim/não)", you should respond `yes para continuar.

c. No assistente de configuração, introduza as definições básicas do interruptor:

- Palavra-passe de administrador
- Mudar nome
- Configuração de gerenciamento fora da banda
- Gateway predefinido
- Serviço SSH (RSA)

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

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

O exemplo a seguir mostra os prompts e as respostas do sistema ao configurar o switch. Os colchetes de ângulo (<<<) mostram onde você insere as informações.

```
---- System Admin Account Setup ----  
Do you want to enforce secure password standard (yes/no) [y]:y  
**<<<**  
  
Enter the password for "admin": password  
Confirm the password for "admin": password  
---- Basic System Configuration Dialog VDC: 1 ----
```

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

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

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

Você insere informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e seleciona SSH com RSA.



Este exemplo mostra as informações mínimas necessárias para configurar o RCF, opções adicionais podem ser configuradas após a aplicação do RCF. Por exemplo, você pode configurar SNMPv3, NTP ou SCP/SFTP depois de aplicar o RCF.

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

O conjunto final de prompts completa a configuração:

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

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

Use this configuration and save it? (yes/no) [y]:

2017 Jun 13 21:24:43 A1 %\$ VDC-1 %\$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

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

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

2. Guardar a configuração:

```
IP_switch-A-1# copy running-config startup-config
```

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

```
IP_switch-A-1# reload
```

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

Transferir e instalar o software Cisco switch NX-os

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

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

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

["NetApp Hardware Universe"](#)

Passos

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

["Transferência do software Cisco"](#)

2. Copie o software do interruptor para o interruptor:

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

Neste exemplo, o arquivo nxos.7.0.3.I4.6.bin e a imagem EPLD são copiados do servidor SFTP 10.10.99.99 para o bootflash local:

```

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

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get    /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                                161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

```

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

dir bootflash:

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

```

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

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

```

4. Instale o software do interruptor:

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

O interruptor recarregará (reiniciará) automaticamente após a instalação do software do interruptor.

O exemplo a seguir mostra a instalação do software em IP_switch_A_1:

```

IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

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

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS [#####] 100%
-- SUCCESS

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

Notifying services about system upgrade. [#####] 100%

```

```
-- SUCCESS
```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

Images will be upgraded according to following table:

Module Required	Image	Running-Version(pri:alt)	New-Version	Upg-
1	nxos	7.0(3)I4(1)	7.0(3)I4(6)	yes
1	bios	v04.24(04/21/2016)	v04.24(04/21/2016)	no

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Performing runtime checks. [#####] 100% --
SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[#####] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#

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

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

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

The switch software is now installed.

6. Verifique se o software do switch foi instalado show version

O exemplo a seguir mostra a saída:

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

.
.
.

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

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

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

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

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

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

  plugin
    Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Atualize a imagem EPLD e reinicie o switch.

```

IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module      Type       Upgradable     Impact      Reason
-----      -----
1           SUP        Yes            disruptive   Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type    EPLD          Running-Version  New-Version  Upg-
Required
-----  -----
1      SUP    MI FPGA        0x07          0x07        No
1      SUP    IO FPGA        0x17          0x19        Yes
1      SUP    MI FPGA2       0x02          0x02        No

The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (      64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module  Type  Upgrade-Result
-----  -----
1      SUP    Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

```

8. após a reinicialização do switch, faça login novamente e verifique se a nova versão do EPLD foi carregada com sucesso.

```
show version module 1 epld
```

9. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Transferir e instalar os ficheiros Cisco IP RCF

Você deve gerar e instalar o arquivo RCF em cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

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

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Se você estiver usando um adaptador QSFP para SFP, talvez seja necessário configurar a porta ISL no modo de velocidade nativo em vez do modo de velocidade de fuga. Consulte a documentação do fornecedor do switch para determinar o modo de velocidade da porta ISL.

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

Interrutor	Ficheiro RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Passos

1. Gerar os arquivos RCF do Cisco para MetroCluster IP.
 - a. Transfira o. "[RcfFileGenerator para MetroCluster IP](#)"
 - b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.



As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:

- a. Copie os arquivos RCF para o primeiro switch:

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

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

```

IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

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

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

dir bootflash:

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

```

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

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

```

4. Configure as regiões TCAM nos switches Cisco 3132Q-V e Cisco 3232C.



Ignore esta etapa se você não tiver switches Cisco 3132Q-V ou Cisco 3232C.

a. No interruptor Cisco 3132Q-V, defina as seguintes regiões TCAM:

```
conf t  
hardware access-list tcam region span 0  
hardware access-list tcam region racl 256  
hardware access-list tcam region e-racl 256  
hardware access-list tcam region qos 256
```

- b. No switch Cisco 3232C, defina as seguintes regiões TCAM:

```
conf t  
hardware access-list tcam region span 0  
hardware access-list tcam region racl-lite 0  
hardware access-list tcam region racl 256  
hardware access-list tcam region e-racl 256  
hardware access-list tcam region qos 256
```

- c. Depois de definir as regiões TCAM, salve a configuração e recarregue o switch:

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

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

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

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

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

Você deve ver saída semelhante ao seguinte:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config  
IP_switch-A-1# copy running-config startup-config
```

7. Recarregue o interruptor:

```
reload
```

```
IP_switch_A_1# reload
```

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

Definição de correção de erro de avanço para sistemas que utilizam conetividade de 25 Gbps

Se o sistema estiver configurado usando conetividade de 25 Gbps, você precisará definir manualmente o parâmetro Correção de erros de Avanço (fec) para Desativado após a aplicação do arquivo RCF. O ficheiro RCF não aplica esta definição.

Sobre esta tarefa

As portas de 25 Gbps devem ser cabeadas antes de executar este procedimento.

["Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C"](#)

Esta tarefa aplica-se apenas a plataformas que utilizam conetividade de 25 Gbps:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Esta tarefa deve ser executada em todos os quatro switches na configuração IP do MetroCluster.

Passos

1. Defina o parâmetro fec como Desligado em cada porta de 25 Gbps conectada a um módulo de controladora e copie a configuração em execução para a configuração de inicialização:
 - a. Entre no modo de configuração: `config t`
 - b. Especifique a interface de 25 Gbps para configurar: `interface interface-ID`
 - c. Defina fec para Off (Desligado): `fec off`
 - d. Repita as etapas anteriores para cada porta de 25 Gbps no switch.
 - e. Sair do modo de configuração: `exit`

O exemplo a seguir mostra os comandos da interface Ethernet1/25/1 no switch IP_switch_A_1:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Repita a etapa anterior nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identificar as portas ISL e os canais de portas não utilizados:

```
show interface brief
```

2. Desative as portas ISL e os canais de portas não utilizados.

Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_1(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configurar criptografia MACsec em switches Cisco 9336C em um site IP MetroCluster



A criptografia MACsec só pode ser aplicada às portas ISL WAN.

Configure a criptografia MACsec em switches Cisco 9336C

Você só deve configurar a criptografia MACsec nas portas ISL WAN executadas entre os sites. Você deve configurar o MACsec depois de aplicar o arquivo RCF correto.

Requisitos de licenciamento para MACsec

MACsec requer uma licença de segurança. Para obter uma explicação completa do esquema de licenciamento do Cisco NX-os e como obter e solicitar licenças, consulte a. "[Guia de licenciamento do Cisco NX-os](#)"

Habilite ISLs WAN de criptografia MACsec Cisco em configurações IP MetroCluster

Você pode ativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config) #
```

2. Ativar MACsec e MKA no dispositivo:

```
feature macsec
```

```
IP_switch_A_1(config) # feature macsec
```

3. Copie a configuração em execução para a configuração de inicialização:

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

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

Configure uma cadeia de chaves e chaves MACsec

Você pode criar uma cadeia de chaves MACsec ou chaves em sua configuração.

Key Lifetime e Hitless Key Rollover

Um chaveiro MACsec pode ter várias chaves pré-compartilhadas (PSKs), cada uma configurada com um ID de chave e uma vida útil opcional. Uma vida útil da chave especifica a hora em que a chave ativa e expira. Na ausência de uma configuração vitalícia, o tempo de vida padrão é ilimitado. Quando uma vida útil é configurada, o MKA passa para a próxima chave pré-compartilhada configurada no chaveiro após a expiração da vida útil. O fuso horário da chave pode ser local ou UTC. O fuso horário padrão é UTC. Uma chave pode rolar para uma segunda chave dentro do mesmo chaveiro se você configurar a segunda chave (no chaveiro) e configurar uma vida útil para a primeira chave. Quando o tempo de vida da primeira tecla expira, ela passa automaticamente para a próxima chave na lista. Se a mesma chave for configurada em ambos os lados do link ao mesmo tempo, a rolagem da chave será sem hitless (ou seja, a chave rolará sem interrupção de tráfego).

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config) #
```

2. Para ocultar a cadeia de carateres octeto de chave criptografada, substitua a cadeia por um caractere curinga na saída show running-config dos comandos e show startup-config:

```
IP_switch_A_1(config) # key-chain macsec-psk no-show
```



A cadeia de carateres octeto também é oculta quando você salva a configuração em um arquivo.

Por padrão, as chaves PSK são exibidas em formato criptografado e podem ser facilmente descriptografadas. Este comando aplica-se apenas às cadeias de chaves MACsec.

3. Crie uma cadeia de chaves MACsec para manter um conjunto de chaves MACsec e entrar no modo de configuração da cadeia de chaves MACsec:

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec  
IP_switch_A_1(config-macseckeychain) #
```

4. Crie uma chave MACsec e entre no modo de configuração da chave MACsec:

```
key key-id
```

O intervalo é de 1 a 32 caracteres de chave de dígitos hexadecimais e o tamanho máximo é de 64 caracteres.

```
IP_switch_A_1 switch(config-macseckeychain) # key 1000  
IP_switch_A_1 (config-macseckeychain-macseckey) #
```

5. Configure a cadeia de carateres octeto para a chave:

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |  
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey) # key-octet-string  
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789  
cryptographic-algorithm AES_256_CMAC
```



O argumento octet-string pode conter até 64 caracteres hexadecimais. A chave octeto é codificada internamente, portanto a chave em texto claro não aparece na saída do show running-config macsec comando.

6. Configure uma vida útil de envio para a chave (em segundos):

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey) # send-lifetime 00:00:00  
Oct 04 2020 duration 100000
```

Por padrão, o dispositivo trata a hora de início como UTC. O argumento de hora de início é a hora do dia e a data em que a chave se torna ativa. O argumento duração é o comprimento do tempo de vida em segundos. A duração máxima é de 2147483646 segundos (aproximadamente 68 anos).

7. Copie a configuração em execução para a configuração de inicialização:

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

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

8. Exibe a configuração do keychain:

```
show key chain name
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configurar uma política MACsec

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config) #
```

2. Criar uma política MACsec:

```
macsec policy name
```

```
IP_switch_A_1(config) # macsec policy abc  
IP_switch_A_1(config-macsec-policy) #
```

3. Configure uma das seguintes cifras, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256:

```
cipher-suite name
```

```
IP_switch_A_1(config-macsec-policy) # cipher-suite GCM-AES-256
```

4. Configure a prioridade do servidor de chaves para quebrar o vínculo entre pares durante uma troca de chaves:

```
key-server-priority number
```

```
switch(config-macsec-policy) # key-server-priority 0
```

5. Configure a política de segurança para definir o processamento de dados e pacotes de controle:

```
security-policy security policy
```

Escolha uma política de segurança das seguintes opções:

- Must-Secure — os pacotes que não transportam cabeçalhos MACsec são descartados

- Should-secure - pacotes que não transportam cabeçalhos MACsec são permitidos (este é o valor padrão)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configure a janela de proteção de repetição para que a interface protegida não aceite um pacote que seja menor do que o tamanho da janela configurado: `window-size number`



O tamanho da janela de proteção de repetição representa o máximo de quadros fora de sequência que o MACsec aceita e não são descartados. O intervalo é de 0 a 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configure o tempo em segundos para forçar um SAK rechavar:

```
sak-expiry-time time
```

Você pode usar este comando para alterar a chave da sessão para um intervalo de tempo previsível. A predefinição é 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configure uma das seguintes compensações de confidencialidade no quadro da camada 2 onde a criptografia começa:

```
conf-offsetconfidentiality offset
```

Escolha entre as seguintes opções:

- CONF-OFFSET-0.
- CONF-OFFSET-30.
- CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```



Esse comando pode ser necessário para que os switches intermediários usem cabeçalhos de pacotes (dmac, smac, etype) como tags MPLS.

9. Copie a configuração em execução para a configuração de inicialização:

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

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

10. Apresentar a configuração da política MACsec:

```
show macsec policy
```

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Ative a criptografia Cisco MACsec nas interfaces

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config) #
```

2. Selecione a interface que você configurou com criptografia MACsec.

Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15  
switch(config-if) #
```

3. Adicione o chaveiro e a política a serem configurados na interface para adicionar a configuração MACsec:

```
macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. Repita as etapas 1 e 2 em todas as interfaces onde a criptografia MACsec deve ser configurada.

5. Copie a configuração em execução para a configuração de inicialização:

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

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

Desative os ISLs de WAN de criptografia Cisco MACsec em configurações IP do MetroCluster

Talvez seja necessário desativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config) #
```

2. Desative a configuração MACsec no dispositivo:

```
macsec shutdown
```

```
IP_switch_A_1(config) # macsec shutdown
```



Selecionar a opção "não" restaura o recurso MACsec.

3. Selecione a interface que você já configurou com o MACsec.

Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

```
IP_switch_A_1(config) # interface ethernet 1/15  
switch(config-if) #
```

4. Remova o chaveiro e a política configurados na interface para remover a configuração MACsec:

```
no macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if) # no macsec keychain 1 policy abc
```

5. Repita as etapas 3 e 4 em todas as interfaces onde o MACsec está configurado.

6. Copie a configuração em execução para a configuração de inicialização:

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

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

Verificando a configuração do MACsec

Passos

1. Repita **All** dos procedimentos anteriores no segundo switch dentro da configuração para estabelecer uma sessão MACsec.
2. Execute os seguintes comandos para verificar se ambos os switches estão criptografados com êxito:
 - a. Executar: `show macsec mka summary`
 - b. Executar: `show macsec mka session`

c. Executar: show macsec mka statistics

Você pode verificar a configuração do MACsec usando os seguintes comandos:

Comando	Exibe informações sobre...
show macsec mka session interface typeslot/port number	A sessão MACsec MKA para uma interface específica ou para todas as interfaces
show key chain name	A configuração da cadeia de chaves
show macsec mka summary	A configuração MACsec MKA
show macsec policy policy-name	A configuração para uma política MACsec específica ou para todas as políticas MACsec

Configurar switches IP NVIDIA

Configurar o switch NVIDIA IP SN2100 para interconexão de cluster e conectividade IP MetroCluster de backend

Você deve configurar os switches IP NVIDIA SN2100 para uso como interconexão de cluster e para conectividade IP MetroCluster de back-end.

Reponha o switch NVIDIA IP SN2100 para os padrões de fábrica

Você pode escolher entre os seguintes métodos para redefinir um switch para as configurações padrão de fábrica.

- [Reponha o interruptor utilizando a opção de ficheiro RCF](#)
- [Baixe e instale o software Cumulus](#)

Reponha o switch usando a opção de arquivo RCF

Antes de instalar uma nova configuração RCF, você deve reverter as configurações do switch NVIDIA.

Sobre esta tarefa

Para restaurar o switch para as configurações padrão, execute o arquivo RCF com a `restoreDefaults` opção. Esta opção copia os ficheiros de cópia de segurança originais para a sua localização original e, em seguida, reinicia o interruptor. Após a reinicialização, o switch fica online com a configuração original que existia quando você executou o arquivo RCF pela primeira vez para configurar o switch.

Os seguintes detalhes de configuração não são redefinidos:

- Configuração de usuário e credencial
- Configuração da porta de rede de gerenciamento, eth0



Todas as outras alterações de configuração que ocorrem durante a aplicação do ficheiro RCF são revertidas para a configuração original.

Antes de começar

- Tem de configurar o interruptor de acordo [Baixe e instale o arquivo NVIDIA RCF](#) com . Se não tiver configurado desta forma ou tiver configurado funcionalidades adicionais antes de executar o ficheiro RCF, não pode utilizar este procedimento.
- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conectado ao switch com uma conexão de console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Verifique se a configuração do RCF foi aplicada com sucesso com a mesma ou uma versão de arquivo RCF compatível e se os arquivos de backup existem.



A saída pode mostrar arquivos de backup, arquivos preservados ou ambos. Se arquivos de backup ou arquivos preservados não aparecerem na saída, você não poderá usar este procedimento.

```

cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
Backup files exist.
Preserved files exist.
Listing completion of the steps:
Success: Step: 1: Performing Backup and Restore
Success: Step: 2: updating MOTD file
Success: Step: 3: Disabling apt-get
Success: Step: 4: Disabling cdp
Success: Step: 5: Adding lldp config
Success: Step: 6: Creating interfaces
Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
Success: Step: 9: Configuring switch basic settings: ecn
Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
Success: Step: 12: Configuring switch basic settings: traffic
classification
Success: Step: 13: Configuring LAG load balancing policies
Success: Step: 14: Configuring the VLAN bridge
Success: Step: 15: Configuring local cluster ISL ports
Success: Step: 16: Configuring MetroCluster ISL ports
Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
Success: Step: 20: Configuring L2FC for MetroCluster interfaces
Success: Step: 21: Configuring the interface to UP
Success: Step: 22: Final commit
Success: Step: 23: Final reboot of the switch
Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Execute o arquivo RCF com a opção para restaurar os padrões: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Responda "sim" ao prompt. O interruptor reverte para a configuração original e reinicializa.
4. Aguarde até que o switch seja reiniciado.

O switch é redefinido e mantém a configuração inicial, como configuração de rede de gerenciamento e credenciais atuais, conforme existiam antes de aplicar o arquivo RCF. Após a reinicialização, você pode aplicar uma nova configuração usando a mesma ou uma versão diferente do arquivo RCF.

Baixe e instale o software Cumulus

Sobre esta tarefa

Siga estas etapas se você quiser redefinir completamente o switch aplicando a imagem Cumulus.

Antes de começar

- Você deve estar conectado ao switch com uma conexão de console serial.
- A imagem do software Cumulus switch é acessível através de HTTP.



Para obter mais informações sobre a instalação do Cumulus Linux, consulte "[Visão geral da instalação e configuração dos switches NVIDIA SN2100](#)"

- Você deve ter a senha raiz para sudo acesso aos comandos.

Passos

1. A partir do download do console Cumulus e coloque em fila a instalação do software do switch com o comando `onie-install -a -i` seguido do caminho do arquivo para o software do switch:

Neste exemplo, o arquivo de firmware `cumulus-linux-4.4.3-mlx-amd64.bin` é copiado do servidor HTTP '50.50.50.50' para o switch local.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
#####
# 100.0%
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
```

```
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/u-boot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
in the future
tar: ..: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
```

```
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N) ? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Responda **y** ao aviso para confirmar a instalação quando a imagem é transferida e verificada.
3. Reinicie o switch para instalar o novo software: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```



O interruptor reinicia e entra na instalação do software do interruptor, o que demora algum tempo. Quando a instalação estiver concluída, o interruptor reinicializa e permanece no prompt de 'login'.

4. Configure as definições básicas do interruptor

- a. Quando o switch é inicializado e no prompt de login, faça login e altere a senha.



O nome de usuário é 'Cumulus' e a senha padrão é 'Cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+c14.4.3u1
(2021-12-18) x86_64
```

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
<http://www.cumulusnetworks.com/support>

The registered trademark Linux (R) is used pursuant to a sublicense from LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide
basis.

cumulus@cumulus:mgmt:~\$

5. Configure a interface de rede de gerenciamento.

Os comandos que você usa dependem da versão do firmware do switch que você está executando.



Os comandos de exemplo a seguir configuram o nome do host como IP_switch_A_1, o endereço IP como 10.10.10.10, a máscara de rede como 255.255.255.0 (24) e o endereço de gateway como 10.10.10.1.

Cumulus 4,4.x

Os comandos de exemplo a seguir configuram o nome do host, endereço IP, máscara de rede e gateway em um switch executando Cumulus 4,4.x.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.

cumulus@cumulus:mgmt:~$ net commit

.
.
.

net add/del commands since the last "net commit"

User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

Cumulus 5,4.x e posterior

Os comandos de exemplo a seguir configuram o nome de host, endereço IP, máscara de rede e gateway em um switch executando Cumulus 5,4.x. ou posterior.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1  
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address  
10.0.10.10/24  
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1  
cumulus@cumulus:mgmt:~$ nv config apply  
cumulus@cumulus:mgmt:~$ nv config save
```

6. Reinicie o switch usando o `sudo reboot` comando.

```
cumulus@cumulus:~$ sudo reboot
```

Quando o switch for reinicializado, você poderá aplicar uma nova configuração usando as etapas em [Baixe e instale o arquivo NVIDIA RCF](#).

Baixe e instale os arquivos RCF do NVIDIA

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

- Você deve ter a senha raiz para `sudo` acesso aos comandos.
- O software do switch está instalado e a rede de gerenciamento está configurada.
- Você seguiu os passos para instalar inicialmente o switch usando o método 1 ou o método 2.
- Você não aplicou nenhuma configuração adicional após a instalação inicial.



Se efetuar uma configuração adicional depois de reiniciar o comutador e antes de aplicar o ficheiro RCF, não poderá utilizar este procedimento.

Sobre esta tarefa

Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster (nova instalação) ou no comutador de substituição (substituição do comutador).

Se você estiver usando um adaptador QSFP para SFP, talvez seja necessário configurar a porta ISL no modo de velocidade nativo em vez do modo de velocidade de fuga. Consulte a documentação do fornecedor do switch para determinar o modo de velocidade da porta ISL.

Passos

1. Gerar os arquivos RCF do NVIDIA para MetroCluster IP.
 - a. Faça download do ["RcfFileGenerator para MetroCluster IP"](#).
 - b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

- c. Navegue para o seu diretório inicial. Se você estiver logado como 'Cumulus', o caminho do arquivo é /home/cumulus.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~  
cumulus@IP_switch_A_1:mgmt:~$ pwd  
/home/cumulus  
cumulus@IP_switch_A_1:mgmt:~$
```

- d. Transfira o ficheiro RCF para este diretório. O exemplo a seguir mostra que você usa SCP para baixar o arquivo SN2100_v2.0.0_IP_switch_A_1.txt do servidor '50.50.50.50' para o diretório principal e salvá-lo como SN2100_v2.0.0_IP_switch_A_1.py:

```
cumulus@Switch-A-1:mgmt:~$ scp  
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt  
./SN2100_v2.0.0_IP_switch-A1.py  
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be  
established.  
RSA key fingerprint is  
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '50.50.50.50' (RSA) to the list of known  
hosts.  
*****  
**  
Banner of the SCP server  
*****  
**  
username@50.50.50's password:  
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00  
cumulus@IP_switch_A_1:mgmt:~$
```

2. Execute o arquivo RCF. O arquivo RCF requer uma opção para aplicar uma ou mais etapas. A menos que instruído pelo suporte técnico, execute o arquivo RCF sem a opção de linha de comando. Para verificar o estado de conclusão dos vários passos do ficheiro RCF, utilize a opção '-1' ou 'All' para aplicar todos os passos (pendentes).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3  
SN2100_v2.0.0_IP_switch_A_1.py  
all  
[sudo] password for cumulus:  
The switch will be rebooted after the step(s) have been run.  
Enter yes or no: yes
```

... the steps will apply - this is generating a lot of output ...

Running Step 24: Final reboot of the switch

... The switch will reboot if all steps applied successfully ...

3. Se a sua configuração utilizar cabos DAC, ative a opção DAC nas portas do switch:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-  
A1.py runCmd <switchport> DacOption [enable | disable]
```

O exemplo a seguir ativa a opção DAC para a porta swp7:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0_Switch-A1.py  
runCmd swp7 DacOption enable  
Running cumulus version : 5.4.0  
Running RCF file version : v2.00  
Running command: Enabling the DacOption for port swp7  
runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0  
runCmd: committed, ret: 0  
Completion: SUCCESS  
cumulus@IP_switch_A_1:mgmt:~$
```

4. Reinicie o switch depois de ativar a opção DAC nas portas do switch:

```
sudo reboot
```



Ao definir a opção DAC para várias portas de switch, você só precisa reiniciar o switch uma vez.

Defina a correção de erro de avanço para sistemas que utilizam conetividade de 25 Gbps

Se o sistema estiver configurado usando conetividade de 25 Gbps, defina manualmente o parâmetro Correção de erros de Avanço (fec) para Desativado após aplicar o RCF. O RCF não aplica esta definição.

Sobre esta tarefa

- Esta tarefa aplica-se apenas a plataformas que utilizam conetividade de 25 Gbps. ["Atribuições de porta de plataforma para switches IP SN2100 compatíveis com NVIDIA"](#) Consulte a .
- Esta tarefa deve ser executada em todos os quatro switches na configuração IP do MetroCluster.
- É necessário atualizar cada porta do switch individualmente, não é possível especificar várias portas ou intervalos de portas no comando.

Passos

1. Defina o fec parâmetro como Desligado para a primeira porta do switch que usa conetividade de 25 Gbps:

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
```

2. Repita a etapa para cada porta de switch de 25 Gbps conectada a um módulo de controlador.

Defina a velocidade da porta do switch para as interfaces IP do MetroCluster

Sobre esta tarefa

- Use este procedimento para definir a velocidade da porta do switch para 100g para os seguintes sistemas:
 - AFF A70, AFF A90, AFF A1K, AFF C80
 - AFF A30, AFF C30, AFF A50, AFF C60
 - FAS50, FAS70, FAS90
- É necessário atualizar cada porta do switch individualmente, não é possível especificar várias portas ou intervalos de portas no comando.

Passo

1. Utilize o ficheiro RCF com a runCmd opção para definir a velocidade. Isso aplica a configuração e salva a configuração.

Os comandos a seguir definem a velocidade para as interfaces MetroCluster swp7 e swp8:

```
sudo python3 SN2100_v2.20_Switch-A1.py runCmd swp7 speed 100
```

```
sudo python3 SN2100_v2.20_Switch-A1.py runCmd swp8 speed 100
```

Exemplo

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd  
swp7 speed 100  
[sudo] password for cumulus: <password>  
    Running cumulus version : 5.4.0  
    Running RCF file version : v2.20  
    Running command: Setting switchport swp7 to 100G speed  
    runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0  
    runCmd: 'nv set interface swp7 link speed 100G', ret: 0  
    runCmd: committed, ret: 0  
    Completion: SUCCESS  
cumulus@Switch-A-1:mgmt:~$
```

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários. Você deve desativar cada canal de porta ou porta individualmente, não é possível especificar várias portas ou intervalos de portas no comando.

Passos

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:



Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

```
net show interface
```

2. Desative as portas ISL e os canais de portas não utilizados usando o arquivo RCF.

```

cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
        sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
Available commands:
    UP / DOWN the switchport
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
    Set the switch port speed
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
    Set the fec mode on the switch port
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
    Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
    Set the option on the port to support DAC cables. This option
does not support port ranges.
        You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
        This setting requires Cumulus 5.4 or a later 5.x release.
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

O seguinte comando de exemplo desativa a porta "swp14":

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Repita esta etapa para cada porta ou canal de porta não utilizado identificado.

Instalar o arquivo de configuração do Ethernet Switch Health Monitor para um switch IP NVIDIA SN2100 MetroCluster

Para configurar o monitoramento de integridade do switch Ethernet em switches Ethernet NVIDIA, siga este procedimento.

Estas instruções se aplicam se os switches NVIDIA X190006-PE e X190006-PI não forem detectados

corretamente, o que pode ser confirmado executando `system switch ethernet show` e verificando se **OTHER** é exibido para o seu modelo. Para identificar o modelo do seu switch NVIDIA, encontre o número da peça com o comando `nv show platform hardware` para NVIDIA CL 5.8 e anteriores ou `nv show platform` para versões posteriores.

 Essas etapas também são recomendadas se você deseja que o monitoramento de integridade e a coleta de logs funcionem conforme o esperado ao usar o NVIDIA CL 5.11.x com as seguintes versões do ONTAP. Embora o monitoramento de integridade e a coleta de logs ainda possam funcionar sem essas etapas, segui-las garante que tudo funcione corretamente.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 e versões de patch posteriores

Antes de começar

- Certifique-se de que o cluster do ONTAP está ativo e em execução.
- Habilite o SSH no switch para usar todos os recursos disponíveis no CSHM.
- Limpe o `/mroot/etc/cshm_nod/nod_sign/` diretório em todos os nós:
 - a. Entre no nodeshell:

```
system node run -node <name>
```

- b. Alterar para privilégios avançados:

```
priv set advanced
```

- c. Liste os arquivos de configuração no `/etc/cshm_nod/nod_sign` diretório. Se o diretório existe e contém arquivos de configuração, ele lista os nomes dos arquivos.

```
ls /etc/cshm_nod/nod_sign
```

- d. Exclua todos os arquivos de configuração correspondentes aos modelos de switch conectados.

Se não tiver a certeza, remova todos os ficheiros de configuração para os modelos suportados listados acima e, em seguida, transfira e instale os ficheiros de configuração mais recentes para esses mesmos modelos.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Confirme se os arquivos de configuração excluídos não estão mais no diretório:

```
ls /etc/cshm_nod/nod_sign
```

Passos

1. Transfira o ficheiro zip de configuração do monitor de integridade do comutador Ethernet com base na versão de lançamento do ONTAP correspondente. Este arquivo está disponível na "[Switches Ethernet NVIDIA](#)" página.
 - a. Na página de download do software NVIDIA SN2100, selecione **Arquivo CSHM NVIDIA**.
 - b. Na página cuidado/deve ler, marque a caixa de seleção para concordar.
 - c. Na página Contrato de Licença de Usuário final, marque a caixa de seleção para concordar e clique em **aceitar e continuar**.

- d. Na página Arquivo CSHM do NVIDIA - Download, selecione o arquivo de configuração aplicável. Estão disponíveis os seguintes ficheiros:

ONTAP 9.15,1 e posterior

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11,1 até 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. carregue o ficheiro zip aplicável para o seu servidor Web interno.
2. Aceda à definição do modo avançado a partir de um dos sistemas ONTAP no cluster.

```
set -privilege advanced
```

3. Execute o comando de configuração do monitor de integridade do switch.

```
cluster1::> system switch ethernet configure-health-monitor
```

4. Verifique se a saída do comando termina com o seguinte texto para sua versão do ONTAP:

ONTAP 9.15,1 e posterior

O monitoramento de integridade do switch Ethernet instalou o arquivo de configuração.

ONTAP 9.11,1 até 9.14.1

SHM instalou o arquivo de configuração.

ONTAP 9.10,1

O pacote baixado do CSHM foi processado com sucesso.

Se ocorrer um erro, contacte o suporte da NetApp.

1. espere até o dobro do intervalo de polling do monitor de integridade do switch Ethernet, encontrado em execução `system switch ethernet polling-interval show`, antes de concluir a próxima etapa.
2. Execute o comando `system switch ethernet configure-health-monitor show` No sistema ONTAP , certifique-se de que os switches do cluster sejam descobertos com o campo monitorado definido como **Verdadeiro** e o campo do número de série não mostrando **Desconhecido**.

```
cluster1::> system switch ethernet configure-health-monitor show
```



Se o seu modelo ainda estiver mostrando **Other** depois de aplicar o arquivo de configuração, entre em Contato com o suporte da NetApp.

Veja o "[switch de sistema ethernet configurar-monitor-de-saúde](#)" comando para mais detalhes.

O que se segue?

["Configurar o monitoramento de integridade do switch"](#).

Monitorar a integridade do switch IP do MetroCluster

Saiba mais sobre o monitoramento da integridade do switch em uma configuração de IP do MetroCluster

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir a integridade operacional dos switches de rede Cluster e Storage e coletar logs de switch para fins de depuração.

Notas importantes para configurar o CSHM em uma configuração de IP do MetroCluster

Esta seção contém as etapas genéricas para configurar SNMPv3 e coleta de logs em switches Cisco, Broadcom e NVIDIA SN2100. Você deve seguir as etapas para uma versão de firmware de switch compatível com uma configuração de IP do MetroCluster. Consulte a seção "["Hardware Universe"](#)" para verificar as versões de firmware suportadas.

Em uma configuração do MetroCluster, você configura o monitoramento de integridade somente nos switches do cluster local.

Para coleta de logs com switches Broadcom e Cisco, um novo usuário deve ser criado no switch para cada cluster com coleta de logs habilitada. Em uma configuração MetroCluster, isso significa que o MetroCluster 1, o MetroCluster 2, o MetroCluster 3 e o MetroCluster 4 exigem a configuração de um usuário separado nos switches. Esses switches não suportam várias chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleção de logs executada substitui quaisquer chaves SSH pré-existentes para o usuário.

Antes de configurar o CSHM, você deve desabilitar ISLs não utilizados para evitar alertas de ISL desnecessários.

Configurar SNMPv3 para monitorar a integridade dos switches IP do MetroCluster

Nas configurações IP do MetroCluster, você pode configurar o SNMPv3 para monitorar a integridade dos switches IP.

Este procedimento mostra as etapas genéricas para configurar o SNMPv3 em um switch. Algumas das versões de firmware de switch listadas podem não ser suportadas em uma configuração de IP do MetroCluster.

Você deve seguir as etapas para uma versão de firmware do switch compatível com uma configuração de IP do MetroCluster. Consulte a "["Hardware Universe"](#)" para verificar as versões de firmware suportadas.

- O SNMPv3 só é suportado no ONTAP 9.12,1 e posterior.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 e versões posteriores corrigem estes dois problemas:
 - "Para monitoramento de integridade ONTAP de switches Cisco, o tráfego SNMPv2 ainda pode ser visto após a mudança para SNMPv3 para monitoramento"
 - "Alertas de energia e ventilador de switch falso-positivos quando ocorrem falhas de SNMP"

Sobre esta tarefa

Os comandos a seguir são usados para configurar um nome de usuário SNMPv3 nos switches **Broadcom**, **Cisco** e **NVIDIA**:

Switches Broadcom

Configure um OPERADOR DE REDE de nome de usuário SNMPv3 em switches Broadcom BES-53248.

- Para **sem autenticação**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Para **MD5/SHA autenticação**:

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Para autenticação **MD5/SHA com criptografia AES/DES**:

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-md5|auth-sha] [priv-aes128|priv-des]
```

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER
```

Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
show snmp status
```

```
(sw1) (Config) # snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1) (Config) # show snmp user snmp

      Name          Group Name      Auth Priv
                  Meth Meth     Remote Engine ID
-----
----->
----->
<username>       network-admin      MD5   AES128
8000113d03d8c497710bee
```

2. Configure o usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshm1!
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>

```

4. Após aguardar o período de pesquisa do CSHM, verifique se o número de série do switch Ethernet está preenchido.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
    Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
    Device Name: sw1
        IP Address: 10.228.136.24
        SNMP Version: SNMPv3
        Is Discovered: true
    DEPRECATED-Community String or SNMPv3 Username: -
        Community String or SNMPv3 Username: <username>
        Model Number: BES-53248
        Switch Network: cluster-network
        Software Version: 3.9.0.2
    Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
    Source Of Switch Version: CDP/ISDP
    Is Monitored ?: true
    Serial Number of the Device: QTFCU3826001C
    RCF Version: v1.8X2 for
Cluster/HA/RDMA

```

Switches Cisco

Configure um nome de usuário SNMPv3 SNMPv3_USER em switches Cisco 9336C-FX2:

- Para **sem autenticação**:

```
snmp-server user SNMPv3_USER NoAuth
```

- Para **MD5/SHA autenticação**:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Para autenticação **MD5/SHA com criptografia AES/DES**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

show snmp user

```
(sw1) (Config) # snmp-server user SNMPv3User auth md5 <auth_password>  
priv aes-128 <priv password>
```

```
(sw1) (Config) # show snmp user
```

SNMP USERS			

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des (no)	network-admin
SNMPv3User	md5	aes-128 (no)	network-operator

NOTIFICATION TARGET USERS (configured for sending V3 Inform)			

User Auth Priv

(sw1) (Config) #

- ## 2. Configure o usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name <username> -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1  
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true  
  
cluster1::*> security login create -user-or-group-name <username>  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshm1!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid

Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Verifique se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
    Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>

```

NVIDIA - CL 5.4.0

Configure um nome de usuário SNMPv3 SNMPv3_USER em switches NVIDIA SN2100 executando CLI 5.4.0:

- Para **sem autenticação**:

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Para **MD5/SHA autenticação**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Para autenticação **MD5/SHA com criptografia AES/DES**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3_USER -application snmp  
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Passos

- Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status  
Simple Network Management Protocol (SNMP) Daemon.  
-----  
Current Status                  active (running)  
Reload Status                   enabled  
Listening IP Addresses         all vrf mgmt  
Main snmpd PID                 4318  
Version 1 and 2c Community String Configured  
Version 3 Usernames            Not Configured  
-----  
cumulus@sw1:~$  
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5  
<password> encrypt-aes <password>  
cumulus@sw1:~$ net commit  
--- /etc/snmp/snmpd.conf          2020-08-02 21:09:34.686949282 +0000  
+++ /run/nclu/snmp/snmpd.conf    2020-08-11 00:13:51.826126655 +0000  
@@ -1,26 +1,28 @@  
# Auto-generated config file: do not edit. #  
agentaddress udp:@mgmt:161  
agentxperms 777 777 snmp snmp  
agentxsocket /var/agentx/master  
createuser _snmptrapusernameX  
+createuser SNMPv3User MD5 <password> AES <password>  
ifmib_max_num_ifaces 500  
iquerysecname _snmptrapusernameX  
master agentx  
monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0  
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```

pass.persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass.persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass.persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass.persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass.persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass.persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass.persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass.persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass.persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass.persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass.persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass.persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
sysservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

User	Timestamp	Command
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username
SNMPv3User		auth-md5 <password> encrypt-aes <password>
cumulus@sw1:~\$		
cumulus@sw1:~\$ net show snmp status		
Simple Network Management Protocol (SNMP) Daemon.		
Current Status		active (running)
Reload Status		enabled
Listening IP Addresses		all vrf mgmt
Main snmpd PID		24253
Version 1 and 2c Community String		Configured
Version 3 Usernames		Configured <---- Configured here
cumulus@sw1:~\$		

2. Configure o usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::>* security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                         Device Name: sw1
(b8:59:9f:09:7c:22)
                                         IP Address: 10.231.80.212
                                         SNMP Version: SNMPv2c
                                         Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
                                         Community String or SNMPv3 Username: cshml!
                                         Model Number: MSN2100-CB2FC
                                         Switch Network: cluster-network
                                         Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                                         Reason For Not Monitoring: None
                                         Source Of Switch Version: LLDP
                                         Is Monitored ?: true
                                         Serial Number of the Device: MT2110X06399 <-----
serial number to check
                                         RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. Verifique se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
    Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
    Device Name: sw1
(b8:59:9f:09:7c:22)
    IP Address: 10.231.80.212
    SNMP Version: SNMPv3
    Is Discovered: true
    DEPRECATED-Community String or SNMPv3 Username: -
        Community String or SNMPv3 Username: SNMPv3User
        Model Number: MSN2100-CB2FC
        Switch Network: cluster-network
        Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
        Reason For Not Monitoring: None
        Source Of Switch Version: LLDP
        Is Monitored ?: true
        Serial Number of the Device: MT2110X06399 <----
serial number to check
    RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LDP Aug-18-2022

```

NVIDIA - CL 5.11.0

Configure um nome de usuário SNMPv3 SNMPv3_USER em switches NVIDIA SN2100 executando CLI 5.11.0:

- Para **sem autenticação**:

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Para **MD5/SHA autenticação**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Para autenticação **MD5/SHA com criptografia AES/DES**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3_USER -application snmp  
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Passos

- Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server  
        applied  
-----  
[username]      SNMPv3_USER  
[username]      limiteduser1  
[username]      testuserauth  
[username]      testuserauthaes  
[username]      testusernoauth  
trap-link-up  
    check-frequency 60  
trap-link-down  
    check-frequency 60  
[listening-address] all  
[readonly-community] $nvsec$94d69b56e921aec1790844eb53e772bf  
state          enabled  
cumulus@sw1:~$
```

- Configure o usuário SNMPv3 no lado ONTAP:

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                         Device Name: sw1
(b8:59:9f:09:7c:22)
                                         IP Address: 10.231.80.212
                                         SNMP Version: SNMPv2c
                                         Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
                                         Community String or SNMPv3 Username: cshm1!
                                         Model Number: MSN2100-CB2FC
                                         Switch Network: cluster-network
                                         Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                                         Reason For Not Monitoring: None
                                         Source Of Switch Version: LLDP
                                         Is Monitored ?: true
                                         Serial Number of the Device: MT2110X06399 <-----
serial number to check
                                         RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

4. Verifique se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
    Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
    Device Name: sw1
(b8:59:9f:09:7c:22)
    IP Address: 10.231.80.212
    SNMP Version: SNMPv3
    Is Discovered: true
    DEPRECATED-Community String or SNMPv3 Username: -
        Community String or SNMPv3 Username: SNMPv3User
        Model Number: MSN2100-CB2FC
        Switch Network: cluster-network
        Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
        Reason For Not Monitoring: None
        Source Of Switch Version: LLDP
        Is Monitored ?: true
        Serial Number of the Device: MT2110X06399 <----
serial number to check
    RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

Configurar coleta de logs em um switch IP do MetroCluster

Em uma configuração de IP do MetroCluster, você pode configurar a coleta de logs para coletar logs de switches para fins de depuração.

 Em switches Broadcom e Cisco, um novo usuário é necessário para cada cluster com coleta de logs. Por exemplo, MetroCluster 1, MetroCluster 2, MetroCluster 3 e MetroCluster 4 exigem a configuração de um usuário separado nos switches. Não há suporte para várias chaves SSH para o mesmo usuário.

Sobre esta tarefa

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir a integridade operacional dos switches de rede Cluster e Storage e coletar logs de switch para fins de depuração. Este procedimento orienta você pelo processo de configuração da coleta, solicitando Registros detalhados de **suporte** e permitindo uma coleta por hora de dados **Periódicos** coletados pela AutoSupport.

NOTA: se você ativar o modo FIPS, você deve concluir o seguinte:



1. Regenerar chaves SSH no switch usando as instruções do fornecedor.
2. Regenerar chaves SSH no ONTAP usando `debug system regenerate-systemshell-key-pair`
3. Execute novamente a rotina de configuração da coleção de logs usando o `system switch ethernet log setup-password` comando

Antes de começar

- O usuário deve ter acesso aos comandos do `switch show`. Se não estiverem disponíveis, crie um novo usuário e conceda as permissões necessárias ao usuário.
- A monitorização do estado do interruptor tem de estar ativada para o interruptor. Verifique isso garantindo que o `Is Monitored:` campo esteja definido como `true` na saída do `system switch ethernet show` comando.
- Para coleta de logs com switches Broadcom e Cisco:
 - O usuário local deve ter privilégios de administrador de rede.
 - Um novo usuário deve ser criado no switch para cada configuração de cluster com a coleção de logs ativada. Esses switches não suportam várias chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleção de logs executada substitui quaisquer chaves SSH pré-existentes para o usuário.
- Para a coleta de logs de suporte com switches NVIDIA, o `user` para coleta de logs deve ter permissão para executar o `cl-support` comando sem ter que fornecer uma senha. Para permitir esse uso, execute o comando:

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus
```

Passos

ONTAP 9.15,1 e posterior

1. Para configurar a coleção de logs, execute o seguinte comando para cada switch. Você será solicitado a digitar o nome do switch, nome de usuário e senha para a coleta de logs.

NOTA: Se responder **y** ao prompt de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias, conforme descrito em [Antes de começar](#).

```
system switch ethernet log setup-password
```

```
cluster1::>*> system switch ethernet log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::>*> system switch ethernet log setup-password
```

```
Enter the switch name: cs1
```

```
Would you like to specify a user other than admin for log collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::>*> system switch ethernet log setup-password
```

```
Enter the switch name: cs2
```

```
Would you like to specify a user other than admin for log collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```



Para CL 5.11.1, crie o usuário **cumulus** e responda **y** ao seguinte prompt: Gostaria de especificar um usuário diferente de admin para coleta de logs? {y|n}: **y**

1. Habilitar coleta periódica de logs:

```
system switch ethernet log modify -device <switch-name> -periodic -enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic  
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs1: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log modify -device cs2 -periodic  
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs2: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	true	scheduled
never-run		
cs2	true	scheduled
never-run		
2 entries were displayed.		

2. Solicitar coleção de logs de suporte:

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device  
cs1
```

cs1: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> system switch ethernet log collect-support-log -device  
cs2
```

cs2: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> *system switch ethernet log show  
Support Periodic Periodic  
Switch Log Enabled Log State  
Log State  
  
cs1 false halted  
initiated  
cs2 true scheduled  
initiated  
2 entries were displayed.
```

3. Para exibir todos os detalhes da coleção de logs, incluindo a habilitação, mensagem de status, carimbo de data/hora anterior e nome do arquivo da coleção periódica, o status da solicitação, a mensagem de status e o carimbo de data/hora e nome do arquivo anterior da coleção de suporte, use o seguinte:

```
system switch ethernet log show -instance
```

```

cluster1::*> system switch ethernet log show -instance

        Switch Name: cs1
        Periodic Log Enabled: true
        Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
        Last Periodic Log Timestamp: 3/11/2024 11:02:59
        Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
        Support Log Requested: false
        Support Log Status: Successfully gathered support logs
- see filename for their location.
        Last Support Log Timestamp: 3/11/2024 11:14:20
        Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

        Switch Name: cs2
        Periodic Log Enabled: false
        Periodic Log Status: Periodic collection has been
halted.
        Last Periodic Log Timestamp: 3/11/2024 11:05:18
        Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
        Support Log Requested: false
        Support Log Status: Successfully gathered support logs
- see filename for their location.
        Last Support Log Timestamp: 3/11/2024 11:18:54
        Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.

```

ONTAP 9.14,1 e anteriores

1. Para configurar a coleção de logs, execute o seguinte comando para cada switch. Você será solicitado a digitar o nome do switch, nome de usuário e senha para a coleta de logs.

OBSERVAÇÃO: se responder **y** ao prompt de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias conforme descrito em [Antes de começar](#).

```
system switch ethernet log setup-password
```

```

cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

```



Para CL 5.11.1, crie o usuário **cumulus** e responda **y** ao seguinte prompt: Gostaria de especificar um usuário diferente de admin para coleta de logs? {y|n}: **y**

1. Para solicitar a coleta de logs de suporte e habilitar a coleta periódica, execute o seguinte comando. Isso inicia ambos os tipos de coleta de log: Os logs detalhados Support e uma coleta de dados por hora Periodic.

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

Aguarde 10 minutos e, em seguida, verifique se a coleção de registos é concluída:

```
system switch ethernet log show
```

 Se algum estado de erro for comunicado pela funcionalidade de recolha de registos (visível na saída do `system switch ethernet log show`), consulte "["Solucionar problemas na coleta de logs"](#)" para obter mais detalhes.

Gerenciar o monitoramento de switches Ethernet em uma configuração IP do MetroCluster

Na maioria dos casos, os switches Ethernet são automaticamente descobertos pelo ONTAP e monitorados pelo CSHM. O arquivo de configuração de referência (RCF) aplicado ao switch, entre outras coisas, ativa o protocolo de descoberta de Cisco (CDP) e/ou o protocolo de descoberta de camada de enlace (LLDP). No entanto, talvez seja necessário adicionar manualmente um switch que não seja descoberto ou remover um switch que não esteja mais em uso. Também pode parar a monitorização ativa mantendo o interruptor na configuração, como durante a manutenção.

Crie uma entrada de switch para que o ONTAP possa monitorá-la

Sobre esta tarefa

Use o `system switch ethernet create` comando para configurar e ativar manualmente o monitoramento de um switch Ethernet especificado. Isso é útil se o ONTAP não adicionar o switch automaticamente ou se você removeu o switch anteriormente e deseja adicioná-lo novamente.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp  
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type  
cluster-network
```

Um exemplo típico é adicionar um switch chamado [deviceName], com endereço IP 1.2.3.4 e credenciais SNMPv2c definidas como **cshm1!**. Use `-type storage-network` em vez de `-type cluster-network` se você estiver configurando um switch de armazenamento.

Desative a monitorização sem eliminar o interruptor

Se você quiser pausar ou parar o monitoramento de um determinado switch, mas ainda mantê-lo para monitoramento futuro, modifique seu `is-monitoring-enabled-admin` parâmetro em vez de excluí-lo.

Por exemplo:

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled  
-admin false
```

Isso permite que você preserve os detalhes e a configuração do switch sem gerar novos alertas ou redescobertas.

Remova um switch que você não precisa mais

Utilize `system switch ethernet delete` para eliminar um interruptor que tenha sido desligado ou que já não seja necessário:

```
system switch ethernet delete -device DeviceName
```

Por padrão, esse comando só será bem-sucedido se o ONTAP não detetar o switch atualmente através do CDP ou do LLDP. Para remover um switch descoberto, use o `-force` parâmetro:

```
system switch ethernet delete -device DeviceName -force
```

`'-force'` Quando o é usado, o switch pode ser readicionado automaticamente se o ONTAP o detetar novamente.

Verificar o monitoramento do switch Ethernet em uma configuração de IP do MetroCluster

O monitor de integridade do switch Ethernet (CSHM) tenta monitorar automaticamente os switches que ele descobre; no entanto, o monitoramento pode não acontecer automaticamente se os switches não estiverem configurados corretamente. Você deve verificar se o monitor de integridade está configurado corretamente para monitorar seus

switches.

Confirme o monitoramento dos switches Ethernet conectados

Sobre esta tarefa

Para confirmar se os switches Ethernet conectados estão sendo monitorados, execute:

```
system switch ethernet show
```

Se a `Model` coluna exibir **OTHER** ou o `IS Monitored` campo exibir **false**, o ONTAP não poderá monitorar o switch. Um valor de **OTHER** normalmente indica que o ONTAP não suporta esse switch para monitoramento de integridade.

O `IS Monitored` campo é definido como **false** pelo motivo especificado no `Reason` campo.

 Se um switch não estiver listado na saída do comando, é provável que o ONTAP não o tenha descoberto. Confirme se o switch está conectado corretamente. Se necessário, você pode adicionar o switch manualmente. Consulte "["Gerenciar o monitoramento de switches Ethernet"](#) para mais detalhes.

Confirme se as versões do firmware e do RCF estão atualizadas

Certifique-se de que o comutador está a executar o firmware suportado mais recente e de que foi aplicado um ficheiro de configuração de referência (RCF) compatível. Mais informações estão disponíveis no "["Página de transferências do suporte da NetApp"](#)".

Por padrão, o monitor de integridade usa SNMPv2c com a string da comunidade **cshm1!** para monitoramento, mas SNMPv3 também pode ser configurado.

Se você precisar alterar a cadeia de caracteres padrão da comunidade SNMPv2c, certifique-se de que a string de comunidade SNMPv2c desejada tenha sido configurada no switch.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c  
-community-or-username newCommunity!
```

 "["Opcional: Configurar SNMPv3"](#)" Consulte para obter detalhes sobre como configurar o SNMPv3 para uso.

Confirme a conexão de rede de gerenciamento

Verifique se a porta de gerenciamento do switch está conectada à rede de gerenciamento.

Uma conexão de porta de gerenciamento correta é necessária para que o ONTAP execute consultas SNMP e coleta de logs.

Informações relacionadas

- ["Solucionar problemas de alertas"](#)

Informações sobre direitos autorais

Copyright © 2026 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 DESTE DOCUMENTO. 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 SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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 DESTE SOFTWARE, 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.