Switches para sistemas ONTAP

Cluster and storage switches

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/pt-br/ontap-systems-switches/index.html on October 03, 2025. Always check docs.netapp.com for the latest.

Índice

Switches para sistemas ONTAP . . . 1
Comece agora . . . 2
O que há de novo para switches . . . 2
Novo suporte do interrutor . . . 2
Saiba mais sobre Cluster, Storage e switches compartilhados . . . 3
Interrutores do cluster . . . 3
Interrutores de armazenamento . . . 3
Switches compartilhados . . . 3
Término da disponibilidade . . . 4
Comece a trabalhar com Cluster, Storage e switches compartilhados . . . 4
Interrutores do cluster . . . 7
BES-53248 com suporte Broadcom . . . 7
Comece agora . . . 7
Instale o hardware . . . 11
Configurar o software . . . 14
Atualize o switch . . . 112
Migrar os switches . . . 156
Substitua os interruptores . . . 192
Cisco Nexus 9336CP-FX2 ou 9336CP-FX2BASE-T . . . 220
Comece agora . . . 220
Instale o hardware . . . 226
Configurar o software . . . 237
Migrar os switches . . . 309
Substitua os interruptores . . . 361
NVIDIA SN2100 . . . 393
Comece agora . . . 393
Instale o hardware . . . 396
Configurar o software . . . 405
Migrar os switches . . . 481
Substitua os interruptores . . . 537
Interrutores de armazenamento . . . 571
Cisco Nexus 9336CP-FX2 ou 9336CP-FX2BASE-T . . . 571
Comece agora . . . 571
Instale o hardware . . . 576
Configurar o software . . . 586
Substituir switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T . . . 630
NVIDIA SN2100 . . . 636
Comece agora . . . 636
Instale o hardware . . . 639
Configure o software . . . 648
Migrar switches . . . 679
Substitua um interrutor de armazenamento NVIDIA SN2100 . . . 690
Switches compartilhados . . . 698

- Cisco Nexus 9336C-FX2 . . . 698
  - Comece agora . . . 698
  - Instale o hardware . . . 700
  - Configurar o software . . . 709
  - Migrar switches . . . 777
  - Substitua um switch compartilhado Cisco Nexus 9336C-FX2 . . . 816
- Monitorar a integridade do interrutor . . . 835
  - Visão geral do monitor de integridade do interrutor . . . 835
  - Configurar o monitoramento de integridade do switch . . . 835
    - Visão geral da configuração . . . 835
    - Configurar a coleção de registos . . . 835
    - Opcional: Configure o SNMPv3 para o seu switch . . . 842
  - Verifique a integridade do interrutor . . . 860
    - Visão geral da verificação de integridade . . . 860
    - Gerenciar o monitoramento de switches Ethernet . . . 860
    - Verifique o monitoramento dos switches Ethernet . . . 862
    - Solucionar problemas de alertas . . . 863
  - Recolha de registos . . . 863
    - Descrição geral da coleção de registos . . . 863
    - Solucionar problemas na coleta de logs . . . 863
- Switches de fim de disponibilidade . . . 865
  - Término da disponibilidade . . . 865
    - Anúncios de fim de venda e fim de vida útil . . . 865
  - Cisco Nexus 3232C . . . 865
    - Comece agora . . . 865
    - Instale o hardware . . . 868
    - Configure o software . . . 878
    - Migrar switches . . . 935
    - Substitua os interrutores . . . 1031
  - Cisco Nexus 3132Q-V . . . 1073
    - Comece agora . . . 1073
    - Instale o hardware . . . 1077
    - Configure o software . . . 1082
    - Migrar switches . . . 1135
    - Substitua os interrutores . . . 1237
  - Cisco Nexus 92300YC . . . 1283
    - Comece agora . . . 1283
    - Instale o hardware . . . 1287
    - Configurar o software . . . 1300
    - Migrar switches . . . 1341
    - Substitua os interrutores . . . 1379
  - NetApp CN1610 . . . 1410
    - Visão geral da instalação e configuração dos switches NetApp CN1610 . . . 1410
    - Instalar e configurar o fluxo de trabalho para os switches NetApp CN1610 . . . 1411
    - Requisitos de documentação para switches NetApp CN1610 . . . 1411

Instalar e configurar . . . 1412
Migrar switches . . . 1448
Substitua os interrutores . . . 1476
Avisos legais . . . 1502
Direitos de autor . . . 1502
Marcas comerciais . . . 1502
Patentes . . . 1502
Política de privacidade . . . 1502

Switches para sistemas ONTAP

Comece agora

O que há de novo para switches

Saiba mais sobre os novos switches para sistemas FAS e AFF. Para obter informações adicionais sobre o interrutor, consulte "NetApp Hardware Universe".

Novo suporte do interrutor

Interrutores	Descrição	Disponível a partir do início
Switch de cluster e armazenamento Cisco Nexus 9336C-FX2-T de 12 portas 10/25/40/100GbE (X190212-CS-PE e X190212-CS-PI)	Suporta configurações de cluster de 10/25/40/100 GbE e configurações de armazenamento de 100 GbE (armazenamento conectado ao switch).	ONTAP 9.10,1
Switch NVIDIA de 16 portas 100GbE (X190006-PE e X190006-PI)	Suporte a switch de interconexão de cluster e switch de storage NVIDIA SN2100, incluindo suporte para configurações IP MetroCluster.	ONTAP 9.10,1
Switch Cisco de 36 portas 100GbE (X190200-CS-PE e X190200-CS-PI)	Dá suporte a uma infraestrutura compartilhada (cluster, HA e storage conectado a switch) no mesmo par de switches Cisco Nexus 9336C-FX2, incluindo suporte para configurações IP MetroCluster.	ONTAP 9.9,1
Switch de 36 portas 100GbE Cisco (X190200-CS-PE e X190200-CS-PI), (X190210-FE-PE e X190210-FE-PI)	Switch de interconexão de cluster Cisco Nexus 9336C-FX2X compatível com switch de storage e switch de storage para sistemas de storage AFF e ASA, bem como para conectividade de dados de front-end.	ONTAP 9,8
Switch Broadcom BES-53248 (X190005 e X190005R)	Suporte para switch de interconexão de cluster BES-53248 Broadcom para controladores AFF/FAS com portas 10/25GbE e 40/100GbE.	ONTAP 9,8

Interrutores	Descrição	Disponível a partir do início
Switch Cisco de 36 portas 100GbE (X190200) e switch Cisco de 32 portas 100GbE (X190100 e X190100R)	Suporte ao switch de storage Cisco Nexus 3232C para conectar compartimentos de unidade NVMe NS224 sistemas de storage AFF e ASA: • AFF A800/AFF ASA A800 • AFF A700/AFF ASA A700 • AFF A400/AFF ASA A400 • AFF A320	ONTAP 9,8

Saiba mais sobre Cluster, Storage e switches compartilhados

O NetApp oferece cluster, storage e switches compartilhados que fornecem comunicações internas com a capacidade de mover dados e interfaces de rede sem interrupções pelo cluster.

Os switches "front-end" fornecem conectividade ao storage de host, enquanto os switches de cluster "back-end" fornecem conexões entre duas ou mais controladoras NetApp.

Somente switches de back-end validados pela NetApp (solicitados pela NetApp) são compatíveis.

Interrutores do cluster

Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós. Os switches de cluster compatíveis com NetApp incluem:

- Broadcom BES-53248
- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Interrutores de armazenamento

Os switches de armazenamento permitem rotear dados entre servidores e matrizes de armazenamento em uma rede de Área de armazenamento (SAN). Os switches de storage compatíveis com NetApp incluem:

- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Switches compartilhados

Os switches compartilhados permitem combinar a funcionalidade de cluster e armazenamento em uma configuração de switch compartilhado, suportando o uso de cluster compartilhado e RCFs de armazenamento. O switch compartilhado suportado pelo NetApp é:

- Cisco Nexus 9336C-FX2

Término da disponibilidade

Os seguintes switches de storage não estão mais disponíveis para compra, mas ainda são compatíveis:

- Cisco Nexus 3232C
- Cisco Nexus 3132Q-V
- Cisco Nexus 92300YC
- NetApp CN1610

Comece a trabalhar com Cluster, Storage e switches compartilhados

Para começar a funcionar com cluster, armazenamento e switches compartilhados, você instala componentes de hardware e configura o switch.

A implantação do switch envolve o seguinte fluxo de trabalho.

Instale o material de fixação do interrutor

Instale seus switches no rack ou gabinete. Acesse as instruções a seguir para o modelo do switch.

	Interrutores do cluster	Interrutores de armazenamento	Switches compartilhados
	• "Instale o interrutor BES-53248" • "Instale o switch Cisco Nexus 9336C-FX2" • "Instale o interrutor NVIDIA SN2100"	• "Instale o switch Cisco Nexus 9336C-FX2" • "Instale o interrutor NVIDIA SN2100"	• "Instale o switch Cisco Nexus 9336C-FX2"

Instale o sistema de storage e as gavetas de storage

Instale seu sistema de armazenamento e prateleiras de armazenamento no gabinete ou rack. Acesse as instruções de instalação e configuração do modelo da sua plataforma.

	• "Sistemas AFF" • "Sistemas ASA" • "Sistemas ASA r2" • "Sistemas FAS"		

Ligue os interrutores aos controladores

As instruções de instalação e configuração dos sistemas ONTAP incluem instruções para o cabeamento das portas da controladora ao switch. No entanto, se você precisar de listas de cabos e transcetores suportados e informações detalhadas sobre as portas do host para o switch, acesse as instruções a seguir para o modelo do switch.

	Interrutores do cluster	Interrutores de armazenamento	Switches compartilhados
	• "Interrutor BES-53248 do cabo" • "Cabo Cisco switch Nexus 9336C-FX2" • "Interrutor do cabo NVIDIA SN2100"	• "Cabo Cisco switch Nexus 9336C-FX2" • "Interrutor do cabo NVIDIA SN2100"	• "Cabo Cisco switch Nexus 9336C-FX2"

Configure o interrutor

Execute uma configuração inicial de seus switches. Acesse as instruções a seguir para o modelo do switch.

	Interrutores do cluster	Interrutores de armazenamento	Switches compartilhados
	• "Configure o switch BES-53248" • "Configurar o switch Cisco Nexus 9336C-FX2" • "Configure o switch NVIDIA SN2100"	• "Configurar o switch Cisco Nexus 9336C-FX2" • "Configure o switch NVIDIA SN2100"	• "Configurar o switch Cisco Nexus 9336C-FX2"

Instale o software do interrutor

Para instalar e configurar o software no switch, siga o fluxo de trabalho de instalação do software para o modelo do switch.

	Interrutores do cluster	Interrutores de armazenamento	Switches compartilhados
	• "Instale o software para os switches BES-53248" • "Instale o software para o switch Cisco Nexus 9336C-FX2" • "Instale o software para o switch NVIDIA SN2100"	• "Instale o software para o switch Cisco Nexus 9336C-FX2" • "Instale o software para o switch NVIDIA SN2100"	• "Instale o software para o switch Cisco Nexus 9336C-FX2"

Conclua a configuração do sistema

Depois de configurar os switches e instalar o software necessário, acesse as instruções de instalação e configuração do modelo da plataforma de sistemas ONTAP para concluir a configuração do sistema.

	• "Sistemas AFF" • "Sistemas ASA" • "Sistemas ASA r2" • "Sistemas FAS"		

7 Concluir a configuração do ONTAP

Depois de instalar e configurar os controladores e switches dos sistemas ONTAP, você deverá concluir a configuração do storage no ONTAP. Acesse as instruções a seguir de acordo com a configuração de implantação.

- Para implantações do ONTAP, "Configurar o ONTAP" consulte .
- Para implantações do ONTAP com MetroCluster, "Configure o MetroCluster com o ONTAP" consulte .

Interrutores do cluster

BES-53248 com suporte Broadcom

Comece agora

Fluxo de trabalho de instalação e configuração para switches BES-53248

O BES-53248 é um switch bare metal projetado para funcionar em clusters ONTAP que variam de dois a 24 nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches BES-53248.

1. **"Revise os requisitos de configuração"**
Revise os requisitos de configuração para o switch de cluster BES-53248.

2. **"Revise os componentes e números de peça"**
Revise os componentes e números de peça do switch de cluster BES-53248.

3. **"Revise a documentação necessária"**
Revise a documentação específica do switch e do controlador para configurar seus switches BES-53248 e o cluster ONTAP .

4. **"Instale o hardware"**
Instale o hardware do switch.

5. **"Configurar o software"**
Configure o software do switch.

Requisitos de configuração para switches de cluster BES-53248

Para instalação e manutenção do switch BES-53248, certifique-se de rever os requisitos de suporte e configuração do EFOS e ONTAP.

Suporte a EFOS e ONTAP

Consulte "NetApp Hardware Universe" e "Matriz de compatibilidade de switches Broadcom" para obter informações de compatibilidade EFOS e ONTAP com os switches BES-53248. O suporte para EFOS e ONTAP pode variar de acordo com o tipo de máquina específico do switch BES-53248. Para obter detalhes sobre todos os tipos de máquinas de comutação BES-52348, "Componentes e números de peça para comutadores de cluster BES-53248"consulte .

Requisitos de configuração

Para configurar um cluster, é necessário o número e o tipo apropriados de cabos e conetores de cabos para os switches do cluster. Dependendo do tipo de switch de cluster que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído.

Atribuições de portas do switch de cluster

Você pode usar a tabela de atribuições de portas de switch de cluster BES-53248 com suporte da Broadcom como guia para configurar seu cluster.

Portas do switch	Utilização de portas
01-16	Nós de porta de cluster 10/25GbE, configuração base
17-48	Nós de porta de cluster 10/25GbE, com licenças
49-54	Nós de porta de cluster 40/100GbE, com licenças, adicionados da direita para a esquerda
55-56	100GbE portas ISL (Inter-Switch Link) de cluster, configuração base

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Restrição de velocidade do grupo de portas

- Nos switches de cluster BES-53248, as portas 48 10/25GbE (37/SFP mais) são combinadas em 12 grupos de 4 portas da seguinte forma: Portas 1-33, 36-25, 28-29, 20-21, 24-13, 16-17, 8-9, 12-32, 4-5, SFP28-40, 41-44 e 45-48.
- A velocidade da porta SFP28/SFP deve ser a mesma (10GbE ou 25GbE) em todas as portas do grupo de 4 portas.

Requisitos adicionais

- Se você comprar licenças adicionais, consulte "Ative as portas de licenças recentes" para obter detalhes sobre como ativá-las.
- Se o SSH estiver ativo, você deve reativá-lo manualmente depois de executar o comando `erase startup-config` e reiniciar o switch.

O que vem a seguir

"Componentes e números de peça" .

Componentes e números de peça para comutadores de cluster BES-53248

Para instalação e manutenção do comutador BES-53248, certifique-se de que lê a lista de componentes e números de peça.

A tabela a seguir lista o número de peça, a descrição e as versões mínimas EFOS e ONTAP para os componentes do switch de cluster BES-53248, incluindo detalhes do kit de trilho de montagem em rack.

É necessária uma versão EFOS mínima de **3.10.0.3** para os números de peça **X190005-B** e **X190005R-B**.

Número de peça	Descrição	Versão mínima do EFOS	Versão mínima do ONTAP
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX - escape lateral da porta)	3.10.0.3	9,8
X190005R-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PSIN (PSIN - Entrada lateral da porta)	3.10.0.3	9,8
X190005	BES-53248, CLSW, 16PT10/25GB, PTSX, BRDCM SUPP	3.4.4.6	9.5P8
X190005R	BES-53248, CLSW, 16PT10/25GB, PSIN, SUPP BRDCM	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Kit de calha de montagem em rack Ozeki 4 POST 19"	N/A.	N/A.

Observe as seguintes informações em relação aos tipos de máquina:

Tipo de máquina	Versão mínima do EFOS
BES-53248A1	3.4.4.6
BES-53248A2	3.10.0.3
BES-53248A3	3.10.0.3

Você pode determinar seu tipo de máquina específico usando o comando: `show version`

Mostrar exemplo

```
(cs1)# show version

Switch: cs1

System Description.............................. EFOS, 3.10.0.3, Linux
5.4.2-b4581018, 2016.05.00.07
Machine Type.................................... BES-53248A3
Machine Model................................... BES-53248
Serial Number................................... QTWCU225xxxxx
Part Number..................................... 1IX8BZxxxxx
Maintenance Level............................... a3a
Manufacturer.................................... QTMC
Burned In MAC Address........................... C0:18:50:F4:3x:xx
Software Version................................ 3.10.0.3
Operating System................................ Linux 5.4.2-b4581018
Network Processing Device....................... BCM56873_A0
.
.
.
```

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches de cluster BES-53248

Para instalação e manutenção do switch BES-53248, certifique-se de revisar a documentação específica do switch e do controlador.

Documentação da Broadcom

Para configurar o switch de cluster BES-53248, você precisa dos seguintes documentos disponíveis no site de suporte da Broadcom: "Linha de produtos Broadcom Ethernet Switch"

Título do documento	Descrição
Guia do Administrador do EFOS v3,4.3	Fornece exemplos de como usar o switch BES-53248 em uma rede típica.
EFOS CLI Command Reference v3,4.3	Descreve os comandos de interface de linha de comando (CLI) que você usa para visualizar e configurar o software BES-53248.
Guia de Introdução do EFOS v3,4.3	Fornece informações detalhadas sobre o switch BES-53248.

Título do documento	Descrição
Guia de Referência SNMP EFOS v3,4.3	Fornece exemplos de como usar o switch BES-53248 em uma rede típica.
Parâmetros e valores de escala do EFOS v3,4.3	Descreve os parâmetros de escala padrão com os quais o software EFOS é fornecido e validado nas plataformas suportadas.
EFOS Especificações funcionais v3,4.3	Descreve as especificações do software EFOS nas plataformas suportadas.
Notas de Lançamento do EFOS v3,4.3	Fornece informações específicas sobre o software BES-53248.
Matriz de compatibilidade de rede e gerenciamento de cluster	Fornece informações sobre compatibilidade de rede. A matriz está disponível no site de download do switch BES-53248 em "Switches de cluster Broadcom".

Documentação de sistemas ONTAP e artigos de KB

Para configurar um sistema ONTAP, você precisa dos seguintes documentos no site de suporte da NetApp em "mysupport.NetApp.com" ou no site da base de conhecimento (KB) em "kb.NetApp.com".

Nome	Descrição
"NetApp Hardware Universe"	Descreve os requisitos de energia e local para todo o hardware NetApp, incluindo gabinetes de sistema, e fornece informações sobre os conetores e opções de cabos relevantes a serem usados juntamente com seus números de peça.
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.
ONTAP 9	Fornece informações detalhadas sobre todos os aspetos da versão do ONTAP 9.
Como adicionar licenciamento de porta adicional para o switch BES-53248 compatível com Broadcom	Fornece informações detalhadas sobre a adição de licenças de porta. Vá para "Artigo da KB" .

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches BES-53248

Para instalar e configurar o hardware de um switch de cluster BES-53248, siga estas etapas:

1 **"Instalar o hardware do switch"**

Instalar e configurar o hardware do switch BES-53248.

2 **"Revise o cabeamento e a configuração"**

Revise as considerações de cabeamento e configuração para o switch de cluster BES-53248.

Instale o hardware do switch do cluster BES-53248

Para instalar o hardware BES-53248, consulte a documentação da Broadcom.

Passos

1. Reveja o "requisitos de configuração".
2. Siga as instruções na "Guia de instalação do comutador de cluster BES-53248 compatível com Broadcom".

O que se segue?

"Revise o cabeamento e a configuração" .

Analise as considerações sobre cabeamento e configuração

Antes de configurar seu switch Broadcom BES-53248, revise as seguintes considerações.

Atribuições de switch de porta de cluster

Você pode usar a tabela de atribuições de portas de switch de cluster BES-53248 com suporte da Broadcom como guia para configurar seu cluster.

Portas de comutação	* Uso de portas*
0-16	Nós de porta de cluster 10/25GbE, configuração base
17-48	Nós de porta de cluster 10/25GbE, com licenças
49-54	Nós de porta de cluster 40/100GbE, com licenças, adicionados da direita para a esquerda
55-56	100GbE portas ISL (Inter-Switch Link) de cluster, configuração base

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Restrição de velocidade do grupo de portas

- Nos switches de cluster BES-53248, as portas 48 10/25GbE (37/SFP mais) são combinadas em 12 grupos de 4 portas da seguinte forma: Portas 1-33, 36-25, 28-29, 20-21, 24-13, 16-17, 8-9, 12-32, 4-5, SFP28-40, 41-44 e 45-48.

- A velocidade da porta SFP28/SFP deve ser a mesma (10GbE ou 25GbE) em todas as portas do grupo de 4 portas.
- Se as velocidades em um grupo de 4 portas forem diferentes, as portas do switch não funcionarão corretamente.

Requisitos da FEC

- Para portas 25G com cabos de cobre, consulte a tabela a seguir para obter detalhes.

  Se o lado do controlador for `auto`, o lado do interrutor é definido como FEC 25G.

FAS2820 FEC			**Switch FEC**			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	UP
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP

- Para portas 25G com cabos de fibra/ótica, consulte a tabela a seguir para obter detalhes:

FAS2820 FEC			**Switch FEC**			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	DOWN
fc	**FC-FEC/BASE-R**	**FC-FEC/BASE-R**	**FEC 25G**	**FEC 25G**	**CL-74**	**UP**
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN
none	**none**	**none**	**No FEC**	**FEC Disabled**	**FEC Disabled**	**UP**
none	none	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN

Implementação do Bootarg

Use o seguinte comando para definir a porta 25G FEC como `auto` ou `fc`, conforme necessário:

```
systemshell -node <node> -command sudo sysctl
dev.ice.<X>.requested_fec=<auto/fc>
```

- Quando definido para **`auto`**:
  - A `auto` configuração propaga a a configuração para o hardware imediatamente e não é necessário reinicializar.
  - Se `bootarg.cpk_fec_fc_eXx already exists`, ele é excluído do armazenamento bootarg.
  - Após uma reinicialização, a `auto` configuração permanece no lugar, pois `auto` é a configuração FEC padrão.
- Quando definido para **`fc`**:
  - A `FC-FEC` configuração propaga a a configuração para o hardware imediatamente e nenhuma reinicialização é necessária.
  - Um novo `bootarg.cpk_fec_fc_eXx` é criado com o valor definido como "verdadeiro".
  - Após uma reinicialização, `FC-FEC` a configuração permanece no lugar para o código do driver usar.

Configurar o software

Fluxo de trabalho de instalação de software para switches BES-53248

Para instalar e configurar o software para um switch de cluster BES-53248, siga estas etapas:

1. **"Configure o interrutor"**

Configurar o switch de cluster BES-53248.

2. **"Instale o software EFOS"**

Faça o download e instale o software do sistema operacional de malha Ethernet (EFOS) no switch de cluster BES-53248.

3. **"Instalar licenças para switches de cluster BES-53248"**

Opcionalmente, adicione novas portas comprando e instalando mais licenças. O modelo base do switch é licenciado para 16 10GbE ou 25GbE portas e duas portas 100GbE.

4. **"Instalar o ficheiro de configuração de referência (RCF)"**

Instale ou atualize o RCF no switch de cluster BES-53248 e, em seguida, verifique as portas para uma licença adicional após a aplicação do RCF.

5 **"Ative o SSH nos switches de cluster BES-53248"**

Se você usar os recursos do Monitor de integridade do comutador Ethernet (CSHM) e da coleção de logs, ative o SSH nos switches.

6 **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações do switch do cluster BES-53248.

Configure o switch do cluster BES-53248

Siga estas etapas para executar uma configuração inicial do switch do cluster BES-53248.

Antes de começar

- O hardware está instalado, conforme descrito em "Instale o hardware".
- Você revisou o seguinte:
  - "Requisitos de configuração"
  - "Componentes e números de peça"
  - "Requisitos de documentação"

Sobre os exemplos

Os exemplos nos procedimentos de configuração usam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches NetApp são `cs1` e `cs2`. A atualização começa no segundo switch, *CS2.*
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.
- O nome do IPspace é Cluster.
- O `cluster1::>` prompt indica o nome do cluster.
- As portas de cluster em cada nó são nomeadas e `e0a` `e0b`. Consulte a "NetApp Hardware Universe" para obter as portas de cluster reais suportadas na sua plataforma.
- Os ISLs (links interswitches) suportados para os switches NetApp são as portas 0/55 e 0/56.
- As conexões de nó suportadas para os switches NetApp são as portas 0/1 a 0/16 com licenciamento padrão.
- Os exemplos usam dois nós, mas você pode ter até 24 nós em um cluster.

Passos

1. Conete a porta serial a um host ou porta serial.
2. Conete a porta de gerenciamento (a porta chave RJ-45 no lado esquerdo do switch) à mesma rede onde o servidor TFTP está localizado.
3. No console, defina as configurações de série do lado do host:
   - 115200 baud
   - 8 bits de dados

- 1 bit de paragem
- paridade: nenhuma
- controle de fluxo: nenhum

4. Faça login no switch como `admin` e pressione **Enter** quando for solicitada uma senha. O nome padrão do switch é **routing**. No prompt, digite `enable`. Isso lhe dá acesso ao modo EXEC privilegiado para configuração de switch.

```
User: admin
Password:
(Routing)> enable
Password:
(Routing)#
```

5. Altere o nome do switch para **CS2**.

```
(Routing)# hostname cs2
(cs2)#
```

6. Para definir um endereço de gerenciamento IPv4 ou IPv6 estático para a porta de serviço do switch:

IPv4

A porta de serviço está definida para usar DHCP por padrão. O endereço IP, a máscara de sub-rede e o endereço de gateway padrão são atribuídos automaticamente.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ip <ip-address> <netmask> <gateway>
```

IPv6

A porta de serviço está definida para usar DHCP por padrão. O endereço IP, a máscara de sub-rede e o endereço de gateway padrão são atribuídos automaticamente.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ipv6 <address>
(cs2)# serviceport ipv6 <gateway>
```

1. Verifique os resultados usando o comando:

```
show serviceport
```

```
(cs2)# show serviceport
Interface Status.............................. Up
IP Address..................................... 172.19.2.2
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 172.19.2.254
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe71:123c/64
IPv6 Default Router............................ fe80::20b:45ff:fea9:5dc0
Configured IPv4 Protocol....................... DHCP
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:71:12:3C
```

2. Configure o domínio e o servidor de nomes:

```
ip domain name <domain_name>
ip name server <server_name>
```

```
(cs2)# configure
(cs2)(Config)# ip domain name company.com
(cs2)(Config)# ip name server 10.10.99.1 10.10.99.2
(cs2)(Config)# exit
(cs2)#
```

3. Configure o servidor NTP.

EFOS 3.10.0.3 e posterior

Configure o fuso horário e a sincronização de horário (NTP):

```
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2)(Config)# ntp server 10.99.99.5
(cs2)(Config)# clock timezone -7
(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 e anteriores

Configure o fuso horário e a sincronização de horário (SNTP):

```
sntp client mode <client_mode>
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2)(Config)# sntp client mode unicast
(cs2)(Config)# sntp server 10.99.99.5
(cs2)(Config)# clock timezone -7
(cs2)(Config)# exit
(cs2)#
```

1. Configure a hora manualmente se você não configurou um servidor NTP na etapa anterior.

EFOS 3.10.0.3 e posterior

Configure a hora manualmente.

`clock`

```
(cs2)# configure
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 e anteriores

Configure a hora manualmente.

`clock`

```
(cs2)# configure
(cs2)(Config)# no sntp client mode
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

1. Salve a configuração em execução na configuração de inicialização:

   `write memory`

```
(cs2)# 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!
```

O que se segue?

"Instale o software EFOS".

Instale o software EFOS

Siga estas etapas para instalar o software do sistema operacional de malha Ethernet (EFOS) no switch de cluster BES-53248.

O software EFOS inclui um conjunto de funcionalidades de rede avançadas e protocolos para o desenvolvimento de sistemas de infra-estrutura Ethernet e IP. Esta arquitetura de software é adequada para qualquer dispositivo organizacional de rede usando aplicativos que exigem inspeção ou separação de pacotes minuciosa.

Prepare-se para a instalação

Antes de começar

- Este procedimento só é adequado para novas instalações.
- Faça o download do software Broadcom EFOS aplicável para seus switches de cluster a partir "Suporte ao comutador Ethernet Broadcom" do site.
- Certifique-se de que o "O comutador de cluster BES-53248 está configurado".

Instale o software

Utilize um dos seguintes métodos para instalar o software EFOS:

- Método 1: Instale o EFOS. Use para a maioria dos casos.
- Método 2: Instalar o EFOS no modo ONIE. Use se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS.

Método 1: Instale o EFOS

Execute as seguintes etapas para instalar o software EFOS.

Passos

1. Faça login na porta do console serial do switch ou conete-se com SSH.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda EFOS, licenças e o arquivo RCF.

Mostrar exemplo

Este exemplo verifica se o switch está conetado ao servidor no endereço IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Transfira o ficheiro de imagem para o interrutor.

   Verifique a tabela a seguir para obter informações sobre protocolos de cópia suportados:

Protocolo	* Pré-requisito*
Protocolo de transferência de ficheiros trivial (TFTP)	Nenhum
Protocolo de transferência de ficheiros SSH (SFTP)	Seu pacote de software deve suportar gerenciamento seguro
FTP	Palavra-passe necessária
XMODEM	Nenhum
YMODEM	Nenhum
ZMODEM	Nenhum
Protocolo de cópia segura (SCP)	Seu pacote de software deve suportar gerenciamento seguro
HTTP	Transferências de arquivos baseadas em CLI suportadas em plataformas selecionadas quando um utilitário WGET nativo está disponível
HTTPS	Transferências de arquivos baseadas em CLI suportadas em plataformas selecionadas quando um utilitário WGET nativo está disponível

   Copiar o arquivo de imagem para a imagem ativa significa que, quando você reiniciar, essa imagem estabelece a versão do EFOS em execução. A imagem anterior permanece disponível como cópia de segurança.

Mostrar exemplo

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk active
Remote Password:**

Mode..................................... SFTP
Set Server IP.................................. 172.19.2.1
Path..................................... //tmp/
Filename..................................... EFOS-3.10.0.3.stk
Data Type.................................... Code
Destination Filename......................... active

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


File transfer operation completed successfully.
```

4. Apresentar as imagens de arranque para a configuração ativa e de cópia de segurança:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# 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           3.10.0.3
```

5. Reinicie o switch:

   `reload`

Mostrar exemplo

```
(cs2)# reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully .
Configuration Saved!
System will now restart!
```

6. Inicie sessão novamente e verifique a nova versão do software EFOS:

   `show version`

Mostrar exemplo

```
(cs2)# show version

Switch: 1

System Description..............................  BES-53248A1,
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04
Machine Type....................................  BES-53248A1,
Machine Model...................................  BES-53248
Serial Number...................................  QTFCU38260023
Maintenance Level...............................  A
Manufacturer....................................  0xbc00
Burned In MAC Address...........................  D8:C4:97:71:0F:40
Software Version................................  3.10.0.3
Operating System................................  Linux 4.4.211-
28a6fe76
Network Processing Device.......................  BCM56873_A0
CPLD Version....................................  0xff040c03

Additional Packages.............................  BGP-4
.............................................  QOS
.............................................  Multicast
.............................................  IPv6
.............................................  Routing
.............................................  Data Center
.............................................  OpEN API
.............................................  Prototype Open API
```

7. Conclua a instalação. Siga estes cinco passos para reconfigurar o interrutor:
    a. "Instalar licenças"
    b. "Instale o ficheiro RCF"
    c. "Ativar SSH"
    d. "Ativar a coleção de registos"
    e. "Configure o SNMPv3 para monitoramento"
8. Repita os passos 1 a 7 no interrutor de parceiro.

Método 2: Instalar o EFOS no modo ONIE

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. Conete-se a um console conetado à porta serial do switch.
2. Inicialize o switch no modo de instalação ONIE.

    Durante a inicialização, selecione ONIE quando você vir o prompt.

Mostrar exemplo

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

Mostrar exemplo

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

O switch inicializa no modo de instalação ONIE.

3. 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 continua e as mensagens são impressas no console.

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

4. Configure a interface Ethernet da porta de gerenciamento do switch e adicione a rota usando `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
```

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

   `ping`

   Mostrar exemplo

```
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:/ #
```

6. Instale o novo software do interrutor:

   `ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86_64`

Mostrar exemplo

```
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 instala e, em seguida, reinicia o interrutor. Deixe o switch reiniciar normalmente para a nova versão do EFOS.

7. Faça login e verifique se o novo software do switch está instalado:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# 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        3.10.0.3
(cs2) #
```

8. Conclua a instalação. O switch reinicializa sem nenhuma configuração aplicada e redefine para os padrões de fábrica. Siga estes seis passos para reconfigurar o interrutor:
   a. "Configure o interrutor"
   b. "Instalar licenças"
   c. "Instale o ficheiro RCF"
   d. "Ativar SSH"

e. "Ativar a coleção de registos"

f. "Configure o SNMPv3 para monitoramento"

9. Repita os passos 1 a 8 no interrutor de parceiro.

O que vem a seguir

"Instalar licenças" .

Instale o ficheiro de configuração de referência (RCF) e o ficheiro de licença

A partir do EFOS 3.12.0.1, pode instalar o ficheiro de configuração de referência (RCF) e o ficheiro de licença depois de configurar o comutador de cluster BES-53248.

> Todas as portas são configuradas quando você instala o RCF, mas você precisa instalar sua licença para ativar as portas configuradas.

Rever os requisitos

Antes de começar

Verifique se os seguintes itens estão em vigor:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual, disponível na "Switches de cluster Broadcom" página.
- Uma configuração de inicialização no RCF que reflete as imagens de inicialização desejadas, necessária se você estiver instalando apenas o EFOS e mantendo sua versão atual do RCF. Se você precisar alterar a configuração de inicialização para refletir as imagens de inicialização atuais, você deve fazê-lo antes de reaplicar o RCF para que a versão correta seja instanciada em futuras reinicializações.
- Uma conexão de console ao switch, necessária ao instalar o RCF a partir de um estado padrão de fábrica. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" para limpar a configuração de antemão.

Documentação sugerida

Consulte a tabela de compatibilidade do switch para as versões ONTAP e RCF suportadas. Consulte a "Baixar o software EFOS" página. Note que pode haver dependências de comando entre a sintaxe de comando no RCF e aquela encontrada em versões do EFOS.

Instale o ficheiro de configuração

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches BES-53248 são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-03_clus1, cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.
- O `cluster1::*>` prompt indica o nome do cluster.
- Os exemplos neste procedimento usam quatro nós. Esses nós usam duas portas de interconexão de

cluster 10GbE `e0a` e `e0b`. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Broadcom switch; os comandos ONTAP são usados, a menos que indicado de outra forma.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Antes de instalar uma nova versão de software de switch e RCFs, use o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" . Se você precisar apagar completamente as configurações do switch, então você precisa executar a configuração básica novamente. Você deve estar conetado ao switch usando o console serial porque uma eliminação completa da configuração redefine a configuração da rede de gerenciamento.

Passo 1: Prepare-se para a instalação

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

onde *x* é a duração da janela de manutenção em horas.

A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

O seguinte comando suprime a criação automática de casos por duas horas:

```
cluster1::*> system node autosupport invoke -node \* -type all -message
MAINT=2h
```

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

É apresentado o aviso avançado (*>).

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
cluster1-02/cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
cluster1-03/cdp
            e0a    cs1                       0/4               BES-
53248
            e0b    cs2                       0/4               BES-
53248
cluster1-04/cdp
            e0a    cs1                       0/3               BES-
53248
            e0b    cs2                       0/3               BES-
53248
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0b     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0b     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
```

5. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address          Model
----------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                           cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. Desativar reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Etapa 2: Configurar portas

1. No switch CS2, confirme a lista de portas que estão conetadas aos nós no cluster.

```
show isdp neighbor
```

2. No switch de cluster CS2, encerre as portas conetadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conetadas a nós ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

3. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

4. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se você ainda não fez isso, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração no interrutor CS2 e execute uma configuração básica.

Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado ao switch usando o console serial para apagar as configurações do switch. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" para limpar a configuração de antemão.

Limpar a configuração não exclui licenças.

a. SSH para o switch.

Só prossiga quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para que a configuração seja apagada.

b. Entrar no modo de privilégio:

```
(cs2)> enable
(cs2)#
```

c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior usada, alguns comandos podem gerar um erro se uma configuração específica não estiver presente):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```

```
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDst
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
```

d. Salve a configuração em execução na configuração de inicialização:

```
(cs2)# 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!
```

e. Execute uma reinicialização do switch:

```
(cs2)# reload

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

f. Faça login no switch novamente usando SSH para concluir a instalação do RCF.

7. Grave todas as personalizações que foram feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, definir velocidades de porta ou o modo FEC de codificação forçada.
8. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, HTTP, TFTP, SFTP ou SCP.

   Este exemplo mostra HTTP sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

Mostrar exemplo

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-RCF-v1.12-
Cluster-HA.txt nvram:reference-config

Mode..................................... HTTP
Set Server IP.............................. 172.19.2.1
Path..................................... <ip-to-
webserver>/path/to/
Filename................................. BES-53248-RCF-v1.12-
Cluster-HA.txt
Data Type................................ Unknown

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...
HTTP Unknown file type transfer starting...
Validating configuration script.....
Configuration script validated.
File transfer operation completed successfully.
```

9. Verifique se o script foi baixado e salvo sob o nome do arquivo que você deu:

   `script list`

```
(cs2)# script list

Configuration Script Name                Size(Bytes)  Date of
Modification
---------------------------------------  -----------
--------------------
Reference-config.scr                     2680         2024 05 31
21:54:22
1 configuration script(s) found.
2045 Kbytes free.
```

10. Aplique o script ao switch:

    `script apply`

Mostrar exemplo

```
(cs2)# script apply reference-config.scr

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

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!
...
...
Configuration script 'reference-config.scr' applied.
```

11. Instale o ficheiro de licença.

Mostrar exemplo

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-LIC.dat
nvram:license-key 1
Mode..................................... HTTP
Set Server IP............................ 172.19.2.1
Path..................................... <ip-to-
webserver>/path/to/
Filename................................. BES-53248-LIC.dat
Data Type................................ license

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...

License Key transfer operation completed successfully.

System reboot is required.
(cs2)# 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!

(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
...
...
```

12. Examine a saída do banner a partir do `show clibanner` comando. Você deve ler e seguir estas instruções para verificar a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
(cs2)# show clibanner

Banner Message configured :
=========================
BES-53248 Reference Configuration File v1.12 for Cluster/HA/RDMA

Switch   : BES-53248
Filename : BES-53248-RCF-v1.12-Cluster.txt
Date     : 11-04-2024
Version  : v1.12
Port Usage:
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added
right to left
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
NOTE:
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms
of port speed:
  Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36,
37-40, 41-44, 45-48
  The port speed should be the same (10GbE or 25GbE) across all
ports in a 4-port group
- If additional licenses are purchased, follow the 'Additional Node
Ports
  activated with Licenses' section for instructions
- If SSH is active, it will have to be re-enabled manually after
'erase startup-config'
  command has been executed and the switch rebooted"
```

13. No switch, verifique se as portas licenciadas adicionais aparecem depois que o RCF é aplicado:

```
show port all | exclude Detach
```

Mostrar exemplo

```
(cs2)# show port all | exclude Detach

                Admin     Physical     Physical   Link   Link
LACP   Actor
Intf      Type  Mode      Mode         Status     Status Trap
Mode   Timeout
--------- ------ --------- ------------ ---------- ------ -------
------ --------
0/1             Enable    Auto                    Down   Enable
Enable long
0/2             Enable    Auto                    Down   Enable
Enable long
0/3             Enable    Auto                    Down   Enable
Enable long
0/4             Enable    Auto                    Down   Enable
Enable long
0/5             Enable    Auto                    Down   Enable
Enable long
0/6             Enable    Auto                    Down   Enable
Enable long
0/7             Enable    Auto                    Down   Enable
Enable long
0/8             Enable    Auto                    Down   Enable
Enable long
0/9             Enable    Auto                    Down   Enable
Enable long
0/10            Enable    Auto                    Down   Enable
Enable long
0/11            Enable    Auto                    Down   Enable
Enable long
0/12            Enable    Auto                    Down   Enable
Enable long
0/13            Enable    Auto                    Down   Enable
Enable long
0/14            Enable    Auto                    Down   Enable
Enable long
0/15            Enable    Auto                    Down   Enable
Enable long
0/16            Enable    Auto                    Down   Enable
Enable long
0/49            Enable    40G Full                Down   Enable
Enable long
0/50            Enable    40G Full                Down   Enable
Enable long
```

```
0/51            Enable    100G Full              Down   Enable
Enable long
0/52            Enable    100G Full              Down   Enable
Enable long
0/53            Enable    100G Full              Down   Enable
Enable long
0/54            Enable    100G Full              Down   Enable
Enable long
0/55            Enable    100G Full              Down   Enable
Enable long
0/56            Enable    100G Full              Down   Enable
Enable long
```

14. No switch, verifique se suas alterações foram feitas:

```
show running-config
```

```
(cs2)# show running-config
```

15. Salve a configuração em execução para que ela se torne a configuração de inicialização quando você reiniciar o switch:

```
write memory
```

```
(cs2)# 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!
```

16. Reinicie o switch e verifique se a configuração em execução está correta:

```
reload
```

```
(cs2)# reload

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

System will now restart!
```

17. No switch de cluster CS2, abra as portas conetadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conetadas a nós ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

18. Verifique as portas no switch CS2:

```
show interfaces status all | exclude Detach
```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

19. Verifique a integridade das portas de cluster no cluster.
    a. Verifique se as portas e0b estão ativas e íntegras em todos os nós do cluster:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02


Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Verifique a integridade do switch a partir do cluster:

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2
BES-53248
            e0b    cs2                       0/2
BES-53248
cluster01-2/cdp
            e0a    cs1                       0/1
BES-53248
            e0b    cs2                       0/1
BES-53248
cluster01-3/cdp
            e0a    cs1                       0/4
BES-53248
            e0b    cs2                       0/4
BES-53248
cluster1-04/cdp
            e0a    cs1                       0/3
BES-53248
            e0b    cs2                       0/2
BES-53248
```

20. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address          Model
----------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                           cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. no switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

   O exemplo a seguir usa a saída de exemplo de interface:

   ```
   (cs1)> enable
   (cs1)# configure
   (cs1)(Config)# interface 0/1-0/16
   (cs1)(Interface 0/1-0/16)# shutdown
   ```

2. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch CS2. Isso pode levar alguns segundos.

   ```
   network interface show -role cluster
   ```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current  Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port     Home
----------- ------------------ ---------- ------------------
------------------ -------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01        e0a      false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01        e0b      true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02        e0a      false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02        e0b      true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03        e0a      false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03        e0b      true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04        e0a      false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04        e0b      true
cluster1::*>
```

3. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
```

4. Repita os passos 4 a 19 no interrutor CS1.

5. Ativar a reversão automática nos LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

6. Interrutor de reinicialização CS1. Isso aciona os LIFs de cluster para reverter para suas portas residenciais. Você pode ignorar os eventos de "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
(cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved! System will now restart!
```

Etapa 3: Verifique a configuração

1. No switch CS1, verifique se as portas do switch conetadas às portas do cluster estão **up**:

```
show interfaces status all | exclude Detach
```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

2. Verifique se o ISL entre os interrutores CS1 e CS2 está funcional:

```
show port-channel 1/1
```

Mostrar exemplo

```
(cs1)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port-channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)
Mbr     Device/       Port      Port
Ports   Timeout       Speed     Active
------- ------------- --------- -------
0/55    actor/long    Auto      True
        partner/long
0/56    actor/long    Auto      True
        partner/long
```

3. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0b     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0a     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0b     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0a     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0a     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
```

4. Verifique se o cluster está em bom estado:

   `cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------- -------------------
------------------ -------

cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster01-
02_clus1  none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster01-
02_clus2  none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-02_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
  Local 169.254.1.3 to Remote 169.254.1.6
  Local 169.254.1.3 to Remote 169.254.1.7
  Local 169.254.1.3 to Remote 169.254.3.4
  Local 169.254.1.3 to Remote 169.254.3.5
  Local 169.254.1.3 to Remote 169.254.3.8
  Local 169.254.1.3 to Remote 169.254.3.9
  Local 169.254.1.1 to Remote 169.254.1.6
  Local 169.254.1.1 to Remote 169.254.1.7
  Local 169.254.1.1 to Remote 169.254.3.4
  Local 169.254.1.1 to Remote 169.254.3.5
  Local 169.254.1.1 to Remote 169.254.3.8
  Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

1. Altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Ativar SSH".

Instalar licenças para switches de cluster BES-53248

O modelo base de switch de cluster BES-53248 é licenciado para portas 16 10GbE ou 25GbE e duas portas 100GbE. Você pode adicionar novas portas comprando mais licenças.

Para o EFOS 3,12 e posterior, siga as etapas de instalação em "Instale o ficheiro de configuração de referência (RCF) e o ficheiro de licença".

Reveja as licenças disponíveis

As seguintes licenças estão disponíveis para uso no switch de cluster BES-53248:

Tipo de licença	Detalhes da licença	Versão de firmware suportada
SW-BES-53248A2-8P-2P	Chave de licença Broadcom 8PT-10G25G e 2PT-40G100G, X190005/R	EFOS 3.4.4.6 e posterior
SW-BES-53248A2-8P-1025G	Chave de licença Broadcom 8 porta 10G25G, X190005/R	EFOS 3.4.4.6 e posterior
SW-BES53248A2-6P-40-100G	Chave de licença Broadcom 6 porta 40G100G, X190005/R	EFOS 3.4.4.6 e posterior

Licenças legadas

A tabela a seguir lista as licenças legadas que estavam disponíveis para uso no switch de cluster BES-53248:

Tipo de licença	Detalhes da licença	Versão de firmware suportada
SW-BES-53248A1-G1-8P-LIC	Chave de licença Broadcom 8P 10-25,2P40-100, X190005/R	EFOS 3.4.3.3 e posterior
SW-BES-53248A1-G1-16P-LIC	Chave de licença Broadcom 16P 10-25,4P40-100, X190005/R	EFOS 3.4.3.3 e posterior

Tipo de licença	Detalhes da licença	Versão de firmware suportada
SW-BES-53248A1-G1-24P-LIC	Chave de licença Broadcom 24P 10-25,6P40-100, X190005/R	EFOS 3.4.3.3 e posterior
SW-BES54248-40-100G-LIC	Chave de licença Broadcom 6Port 40G100G, X190005/R	EFOS 3.4.4.6 e posterior
SW-BES53248-8P-10G25G-LIC	Chave de licença Broadcom 8Port 10G25G, X190005/R	EFOS 3.4.4.6 e posterior
SW-BES53248-16P-1025G-LIC	Chave de licença Broadcom 16Port 10G25G, X190005/R	EFOS 3.4.4.6 e posterior
SW-BES53248-24P-1025G-LIC	Chave de licença Broadcom 24Port 10G25G, X190005/R	EFOS 3.4.4.6 e posterior

Não é necessária uma licença para a configuração base.

Instalar ficheiros de licença

Siga estas etapas para instalar licenças para switches de cluster BES-53248.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda EFOS, licenças e o arquivo RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch está conetado ao servidor no endereço IP 172.19.2.1:

   ```
   (cs2)# ping 172.19.2.1
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Verifique a utilização atual da licença no interrutor CS2:

   ```
   show license
   ```

Mostrar exemplo

```
(cs2)# show license
Reboot needed.................................. No
Number of active licenses...................... 0

License Index  License Type     Status
-------------- ---------------- -----------

No license file found.
```

4. Instale o ficheiro de licença.

   Repita esta etapa para carregar mais licenças e usar diferentes números de índice de chave.

   Mostrar exemplo

   O exemplo a seguir usa SFTP para copiar um arquivo de licença para um índice de chave 1.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode........................................... SFTP
Set Server IP.................................. 172.19.2.1
Path........................................... /var/lib/tftpboot/
Filename....................................... license.dat
Data Type...................................... license

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...


License Key transfer operation completed successfully. System reboot
is required.
```

5. Exiba todas as informações atuais da licença e observe o status da licença antes que o switch CS2 seja reinicializado:

   `show license`

Mostrar exemplo

```
(cs2)# show license

Reboot needed.................................. Yes
Number of active licenses...................... 0


License Index  License Type      Status
-------------- ----------------- --------------------------------
1              Port              License valid but not applied
```

6. Exibir todas as portas licenciadas:

   `show port all | exclude Detach`

   As portas dos arquivos de licença adicionais não são exibidas até que o switch seja reinicializado.

Mostrar exemplo

```
(cs2)# show port all | exclude Detach

                Admin     Physical   Physical   Link   Link    LACP
Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ -------
------ --------
0/1             Disable   Auto                  Down   Enable
Enable long
0/2             Disable   Auto                  Down   Enable
Enable long
0/3             Disable   Auto                  Down   Enable
Enable long
0/4             Disable   Auto                  Down   Enable
Enable long
0/5             Disable   Auto                  Down   Enable
Enable long
0/6             Disable   Auto                  Down   Enable
Enable long
0/7             Disable   Auto                  Down   Enable
Enable long
0/8             Disable   Auto                  Down   Enable
Enable long
0/9             Disable   Auto                  Down   Enable
Enable long
0/10            Disable   Auto                  Down   Enable
Enable long
0/11            Disable   Auto                  Down   Enable
Enable long
0/12            Disable   Auto                  Down   Enable
Enable long
0/13            Disable   Auto                  Down   Enable
Enable long
0/14            Disable   Auto                  Down   Enable
Enable long
0/15            Disable   Auto                  Down   Enable
Enable long
0/16            Disable   Auto                  Down   Enable
Enable long
0/55            Disable   Auto                  Down   Enable
Enable long
0/56            Disable   Auto                  Down   Enable
Enable long
```

7. Reinicie o switch:

   `reload`

   Mostrar exemplo

   ```
   (cs2)# reload

   The system has unsaved changes.
   Would you like to save them now? (y/n) y

   Config file 'startup-config' created successfully .

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

8. Verifique se a nova licença está ativa e observe que a licença foi aplicada:

   `show license`

   Mostrar exemplo

   ```
   (cs2)# show license

   Reboot needed.................................. No
   Number of installed licenses................... 1
   Total Downlink Ports enabled................... 16
   Total Uplink Ports enabled..................... 8

   License Index  License Type              Status
   -------------- ------------------------
   ----------------------------------
   1              Port                      License applied
   ```

9. Verifique se todas as novas portas estão disponíveis:

   `show port all | exclude Detach`

Mostrar exemplo

```
(cs2)# show port all | exclude Detach

                Admin     Physical   Physical   Link   Link    LACP
Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ -------
------ --------
0/1             Disable    Auto                Down   Enable
Enable long
0/2             Disable    Auto                Down   Enable
Enable long
0/3             Disable    Auto                Down   Enable
Enable long
0/4             Disable    Auto                Down   Enable
Enable long
0/5             Disable    Auto                Down   Enable
Enable long
0/6             Disable    Auto                Down   Enable
Enable long
0/7             Disable    Auto                Down   Enable
Enable long
0/8             Disable    Auto                Down   Enable
Enable long
0/9             Disable    Auto                Down   Enable
Enable long
0/10            Disable    Auto                Down   Enable
Enable long
0/11            Disable    Auto                Down   Enable
Enable long
0/12            Disable    Auto                Down   Enable
Enable long
0/13            Disable    Auto                Down   Enable
Enable long
0/14            Disable    Auto                Down   Enable
Enable long
0/15            Disable    Auto                Down   Enable
Enable long
0/16            Disable    Auto                Down   Enable
Enable long
0/49            Disable   100G Full            Down   Enable
Enable long
0/50            Disable   100G Full            Down   Enable
Enable long
```

```
0/51              Disable   100G Full              Down   Enable
Enable long
0/52              Disable   100G Full              Down   Enable
Enable long
0/53              Disable   100G Full              Down   Enable
Enable long
0/54              Disable   100G Full              Down   Enable
Enable long
0/55              Disable   100G Full              Down   Enable
Enable long
0/56              Disable   100G Full              Down   Enable
Enable long
```

Ao instalar licenças adicionais, você deve configurar as novas interfaces manualmente. Não volte a aplicar um RCF a um interrutor de produção em funcionamento existente.

Solucionar problemas de instalação

Quando surgirem problemas ao instalar uma licença, execute os seguintes comandos de depuração antes de executar o `copy` comando novamente.

Depurar comandos para usar: `debug transfer` E. `debug license`

Mostrar exemplo

```
(cs2)# debug transfer
Debug transfer output is enabled.
(cs2)# debug license
Enabled capability licensing debugging.
```

Quando você executa o `copy` comando com `debug transfer` as opções e `debug license` ativadas, a saída do log é retornada.

Mostrar exemplo

```
transfer.c(3083):Transfer process  key or certificate file type = 43
transfer.c(3229):Transfer process  key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
LICENSING :
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
  },
  "description": "",
  "ports": "0+6"
  }
}.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Model BES-53248
matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Applying license file
1.
```

Verifique o seguinte na saída de depuração:

- Verifique se o número de série corresponde: `Serial number QTFCU38290012 matched.`
- Verifique se o modelo do interrutor corresponde: `Model BES-53248 matched.`
- Verifique se o índice de licença especificado não foi usado anteriormente. Quando um índice de licença já é usado, o seguinte erro é retornado: `License file /mnt/download//license.dat.1 already exists.`
- Uma licença de porta não é uma licença de recurso. Portanto, a seguinte declaração é esperada: `Feature not found in license file with index = 1.`

Use o `copy` comando para fazer backup de licenças de porta para o servidor:

```
(cs2)# copy nvram:license-key 1
scp://<UserName>@<IP_address>/saved_license_1.dat
```

Se você precisar fazer o downgrade do software do switch da versão 3,4.4,6, as licenças serão removidas. Este é o comportamento esperado.

Você deve instalar uma licença mais antiga apropriada antes de reverter para uma versão mais antiga do software.

Ative portas recém-licenciadas

Para ativar portas recém-licenciadas, você precisa editar a versão mais recente do RCF e descomentar os detalhes da porta aplicável.

A licença padrão ativa as portas 0/1 a 0/16 e 0/55 a 0/56 enquanto as portas recém-licenciadas estarão entre as portas 0/17 a 0/54, dependendo do tipo e do número de licenças disponíveis. Por exemplo, para ativar a licença SW-BES54248-40-100g-LIC, você deve descomentar a seguinte seção no RCF:

Mostrar exemplo

```
.
.
!
! 2-port or 6-port 40/100GbE node port license block
!
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
.
.
```

Para portas de alta velocidade entre 0/49 e 0/54 inclusive, descomente cada porta, mas apenas descomente uma linha **speed** no RCF para cada uma dessas portas, seja: **Speed 100g full-duplex** ou **speed 40G full-duplex** como mostrado no exemplo. Para portas de baixa velocidade entre 0/17 e 0/48 inclusive, descomente toda a seção de 8 portas quando uma licença apropriada tiver sido ativada.

O que se segue?

"Instalar o ficheiro de configuração de referência (RCF)" ou "Atualize o RCF".

Instalar o ficheiro de configuração de referência (RCF)

Pode instalar o ficheiro de configuração de referência (RCF) depois de configurar a central de cluster BES-53248 e depois de aplicar as novas licenças.

Para o EFOS 3,12 e posterior, siga as etapas de instalação em "Instale o ficheiro de configuração de referência (RCF) e o ficheiro de licença".

Rever os requisitos

Antes de começar

Verifique se os seguintes itens estão em vigor:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O arquivo RCF atual, disponível na "Switches de cluster Broadcom" página.
- Uma configuração de inicialização no RCF que reflete as imagens de inicialização desejadas, necessária se você estiver instalando apenas o EFOS e mantendo sua versão atual do RCF. Se você precisar alterar a configuração de inicialização para refletir as imagens de inicialização atuais, você deve fazê-lo antes de reaplicar o RCF para que a versão correta seja instanciada em futuras reinicializações.
- Uma conexão de console ao switch, necessária ao instalar o RCF a partir de um estado padrão de fábrica. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" para limpar a configuração de antemão.

Documentação sugerida

Consulte a tabela de compatibilidade do switch para as versões ONTAP e RCF suportadas. Consulte a "Baixar o software EFOS" página. Note que pode haver dependências de comando entre a sintaxe de comando no RCF e aquela encontrada em versões do EFOS.

Instale o ficheiro de configuração

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches BES-53248 são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-03_clus1, cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.
- O `cluster1::*>` prompt indica o nome do cluster.
- Os exemplos neste procedimento usam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE `e0a` e `e0b`. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Broadcom switch; os comandos ONTAP são usados, a menos que indicado de outra forma.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Antes de instalar uma nova versão de software de switch e RCFs, use o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" . Se você precisar apagar completamente as configurações do switch, então você precisa executar a configuração básica novamente. Você deve estar conetado ao switch usando o console serial porque uma eliminação completa da configuração redefine a configuração da rede de gerenciamento.

Passo 1: Prepare-se para a instalação

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde *x* é a duração da janela de manutenção em horas.

   A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   O seguinte comando suprime a criação automática de casos por duas horas:

```
cluster1::*> system node autosupport invoke -node \* -type all -message
MAINT=2h
```

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

É apresentado o aviso avançado (*>).

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
cluster1-02/cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
cluster1-03/cdp
            e0a    cs1                       0/4               BES-
53248
            e0b    cs2                       0/4               BES-
53248
cluster1-04/cdp
            e0a    cs1                       0/3               BES-
53248
            e0b    cs2                       0/3               BES-
53248
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0b     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0b     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
```

5. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address          Model
----------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                           cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. Desativar reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Etapa 2: Configurar portas

1. No switch CS2, confirme a lista de portas que estão conetadas aos nós no cluster.

```
show isdp neighbor
```

2. No switch de cluster CS2, encerre as portas conetadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conetadas a nós ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

3. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

4. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se você ainda não fez isso, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração no interrutor CS2 e execute uma configuração básica.

Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado ao switch usando o console serial para apagar as configurações do switch. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" para limpar a configuração de antemão.

Limpar a configuração não exclui licenças.

a. SSH para o switch.

Só prossiga quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para que a configuração seja apagada.

b. Entrar no modo de privilégio:

```
(cs2)> enable
(cs2)#
```

c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior usada, alguns comandos podem gerar um erro se uma configuração específica não estiver presente):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no class-map CLUSTER
no class-map HA
no class-map RDMA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
```

d. Salve a configuração em execução na configuração de inicialização:

```
(cs2)# 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!
```

e. Execute uma reinicialização do switch:

```
(cs2)# reload

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

f. Faça login no switch novamente usando SSH para concluir a instalação do RCF.

7. Observe o seguinte:

a. Se tiverem sido instaladas licenças de porta adicionais no switch, você deverá modificar o RCF para configurar as portas licenciadas adicionais. "Ative portas recém-licenciadas"Consulte para obter detalhes.

b. Grave todas as personalizações que foram feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, definir velocidades de porta ou o modo FEC de codificação forçada.

EFOS versão 3,12.x e posterior

1. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Este exemplo mostra que o SFTP está sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
(cs2)# copy tftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..................................... TFTP
Set Server IP.................................. 172.19.2.1
Path..................................... /
Filename..................................... BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type.................................... Config Script
Destination Filename.......................... reference-config.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifique se o script foi baixado e salvo sob o nome do arquivo que você deu:

   `script list`

```
(cs2)# script list

Configuration Script Name                  Size(Bytes)  Date of
Modification
---------------------------------------  -----------
--------------------
reference-config.scr                       2680         2024 05 31
21:54:22
2 configuration script(s) found.
2042 Kbytes free.
```

2. Aplique o script ao switch:

   `script apply`

```
(cs2)# script apply reference-config.scr

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

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'reference-config.scr' applied.
```

Todas as outras versões do EFOS

1. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Este exemplo mostra que o SFTP está sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt
nvram:script BES-53248_RCF_v1.9-Cluster-HA.scr
Remote Password:**
Mode..................................... SFTP
Set Server IP.............................. 172.19.2.1
Path..................................... //tmp/
Filename................................. BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type................................ Config Script
Destination Filename..................... BES-53248_RCF_v1.9-
Cluster-HA.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifique se o script foi baixado e salvo no nome do arquivo que você deu:

   ```
   script list
   ```

```
(cs2)# script list

Configuration Script Name                    Size(Bytes)  Date of
Modification
-----------------------------------------  -----------
--------------------
BES-53248_RCF_v1.9-Cluster-HA.scr          2241         2020 09 30
05:41:00

1 configuration script(s) found.
```

2. Aplique o script ao switch:

   `script apply`

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.scr

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

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. Examine a saída do banner a partir do `show clibanner` comando. Você deve ler e seguir estas instruções para verificar a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
(cs2)# show clibanner

Banner Message configured :
=========================
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA

Switch   : BES-53248
Filename : BES-53248-RCF-v1.9-Cluster.txt
Date     : 10-26-2022
Version  : v1.9
Port Usage:
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added
right to left
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
NOTE:
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms
of port
speed:
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-
40, 41-44,
45-48
The port speed should be the same (10GbE or 25GbE) across all ports
in a 4-port
group
- If additional licenses are purchased, follow the 'Additional Node
Ports
activated with Licenses' section for instructions
- If SSH is active, it will have to be re-enabled manually after
'erase
startup-config'
command has been executed and the switch rebooted
```

2. No switch, verifique se as portas licenciadas adicionais aparecem depois que o RCF é aplicado:

```
show port all | exclude Detach
```

Mostrar exemplo

```
(cs2)# show port all | exclude Detach

                Admin     Physical     Physical   Link   Link
LACP   Actor
Intf      Type  Mode      Mode         Status     Status Trap
Mode   Timeout
--------- ------ --------- ------------ ---------- ------ -------
------ --------
0/1             Enable    Auto                    Down   Enable
Enable long
0/2             Enable    Auto                    Down   Enable
Enable long
0/3             Enable    Auto                    Down   Enable
Enable long
0/4             Enable    Auto                    Down   Enable
Enable long
0/5             Enable    Auto                    Down   Enable
Enable long
0/6             Enable    Auto                    Down   Enable
Enable long
0/7             Enable    Auto                    Down   Enable
Enable long
0/8             Enable    Auto                    Down   Enable
Enable long
0/9             Enable    Auto                    Down   Enable
Enable long
0/10            Enable    Auto                    Down   Enable
Enable long
0/11            Enable    Auto                    Down   Enable
Enable long
0/12            Enable    Auto                    Down   Enable
Enable long
0/13            Enable    Auto                    Down   Enable
Enable long
0/14            Enable    Auto                    Down   Enable
Enable long
0/15            Enable    Auto                    Down   Enable
Enable long
0/16            Enable    Auto                    Down   Enable
Enable long
0/49            Enable    40G Full                Down   Enable
Enable long
0/50            Enable    40G Full                Down   Enable
Enable long
```

```
0/51            Enable    100G Full              Down   Enable
Enable long
0/52            Enable    100G Full              Down   Enable
Enable long
0/53            Enable    100G Full              Down   Enable
Enable long
0/54            Enable    100G Full              Down   Enable
Enable long
0/55            Enable    100G Full              Down   Enable
Enable long
0/56            Enable    100G Full              Down   Enable
Enable long
```

3. Verifique no switch se suas alterações foram feitas:

```
show running-config
```

```
(cs2)# show running-config
```

4. Salve a configuração em execução para que ela se torne a configuração de inicialização quando você reiniciar o switch:

```
write memory
```

```
(cs2)# 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!
```

5. Reinicie o switch e verifique se a configuração em execução está correta:

```
reload
```

```
(cs2)# reload

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

System will now restart!
```

6. No switch de cluster CS2, abra as portas conetadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conetadas a nós ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

7. Verifique as portas no switch CS2:

```
show interfaces status all | exclude Detach
```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

8. Verifique a integridade das portas de cluster no cluster.
   a. Verifique se as portas e0b estão ativas e íntegras em todos os nós do cluster:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02


Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Verifique a integridade do switch a partir do cluster:

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2
BES-53248
            e0b    cs2                       0/2
BES-53248
cluster01-2/cdp
            e0a    cs1                       0/1
BES-53248
            e0b    cs2                       0/1
BES-53248
cluster01-3/cdp
            e0a    cs1                       0/4
BES-53248
            e0b    cs2                       0/4
BES-53248
cluster1-04/cdp
            e0a    cs1                       0/3
BES-53248
            e0b    cs2                       0/2
BES-53248
```

9. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address          Model
----------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                           cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. no switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

   O exemplo a seguir usa a saída de exemplo de interface:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# shutdown
```

2. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch CS2. Isso pode levar alguns segundos.

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current  Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port     Home
----------- ------------------ ---------- ------------------
-----------------  -------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01        e0a      false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01        e0b      true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02        e0a      false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02        e0b      true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03        e0a      false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03        e0b      true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04        e0a      false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04        e0b      true
cluster1::*>
```

3. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
```

4. Repita os passos 4 a 19 no interrutor CS1.

5. Ativar a reversão automática nos LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

6. Interrutor de reinicialização CS1. Isso aciona os LIFs de cluster para reverter para suas portas residenciais. Você pode ignorar os eventos de "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
(cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved! System will now restart!
```

Etapa 3: Verifique a configuração

1. No switch CS1, verifique se as portas do switch conetadas às portas do cluster estão **up**:

```
show interfaces status all | exclude Detach
```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

2. Verifique se o ISL entre os interrutores CS1 e CS2 está funcional:

```
show port-channel 1/1
```

Mostrar exemplo

```
(cs1)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port-channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)
Mbr     Device/       Port      Port
Ports   Timeout       Speed     Active
------- ------------- --------- -------
0/55    actor/long    Auto      True
        partner/long
0/56    actor/long    Auto      True
        partner/long
```

3. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0b     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0a     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0b     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0a     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0a     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
```

4. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------- -------------------
------------------ -------

cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster01-
02_clus1  none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster01-
02_clus2  none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-02_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
  Local 169.254.1.3 to Remote 169.254.1.6
  Local 169.254.1.3 to Remote 169.254.1.7
  Local 169.254.1.3 to Remote 169.254.3.4
  Local 169.254.1.3 to Remote 169.254.3.5
  Local 169.254.1.3 to Remote 169.254.3.8
  Local 169.254.1.3 to Remote 169.254.3.9
  Local 169.254.1.1 to Remote 169.254.1.6
  Local 169.254.1.1 to Remote 169.254.1.7
  Local 169.254.1.1 to Remote 169.254.3.4
  Local 169.254.1.1 to Remote 169.254.3.5
  Local 169.254.1.1 to Remote 169.254.3.8
  Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

1. Altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Ativar SSH".

Ative o SSH nos switches de cluster BES-53248

Se você estiver usando os recursos do Monitor de integridade do comutador Ethernet (CSHM) e da coleção de logs, será necessário gerar as chaves SSH e, em seguida, ativar o SSH nos switches do cluster.

Passos

1. Verifique se o SSH está desativado:

   ```
   show ip ssh
   ```

   Mostrar exemplo

   ```
   (switch)# show ip ssh

   SSH Configuration

   Administrative Mode: ......................... Disabled
   SSH Port: ..................................... 22
   Protocol Level: ............................... Version 2
   SSH Sessions Currently Active: ................ 0
   Max SSH Sessions Allowed: ..................... 5
   SSH Timeout (mins): ........................... 5
   Keys Present: ................................. DSA(1024) RSA(1024)
   ECDSA(521)
   Key Generation In Progress: ................... None
   SSH Public Key Authentication Mode: ........... Disabled
   SCP server Administrative Mode: ............... Disabled
   ```

   - Se o SSH não estiver desabilitado, desabilite-o da seguinte maneira:

     ```
     no ip ssh server enable

     no ip scp server enable
     ```

     - Para EFOS 3.12 e posteriores, o acesso ao console é necessário, pois as sessões SSH ativas são perdidas quando o SSH é desabilitado.
     - Para EFOS 3.11 e versões anteriores, as sessões SSH atuais são mantidas abertas após a desativação do servidor SSH.

+

> Certifique-se de desabilitar o SSH antes de modificar as chaves, caso contrário, um aviso será reportado no switch.

2. No modo de configuração, gere as chaves SSH:

   `crypto key generate`

   Mostrar exemplo

   ```
   (switch)# config

   (switch) (Config)# crypto key generate rsa

   Do you want to overwrite the existing RSA keys? (y/n): y


   (switch) (Config)# crypto key generate dsa

   Do you want to overwrite the existing DSA keys? (y/n): y


   (switch) (Config)# crypto key generate ecdsa 521

   Do you want to overwrite the existing ECDSA keys? (y/n): y
   ```

3. No modo de configuração, defina a autorização AAA para coleta de logs ONTAP :

   `aaa authorization commands "noCmdAuthList" none`

   Mostrar exemplo

   ```
   (switch) (Config)# aaa authorization commands "noCmdAuthList" none
   (switch) (Config)# exit
   ```

4. Reative o SSH/SCP.

Mostrar exemplo

```
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
```

5. Salve essas alterações no startup-config:

   `write memory`

   Mostrar exemplo

```
(switch)# 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!
```

6. Encripte as chaves SSH (apenas para o modo **FIPS**):

   No modo FIPS, as chaves devem ser criptografadas com uma senha para segurança. Na ausência de uma chave criptografada, o aplicativo não inicia. As chaves são criadas e criptografadas usando os seguintes comandos:

Mostrar exemplo

```
(switch) configure
(switch) (Config)# crypto key encrypt write rsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch) (Config)# crypto key encrypt write dsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch)(Config)# crypto key encrypt write ecdsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch) (Config)# end
(switch)# 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!
```

7. Reinicie o switch:

```
reload
```

8. Verifique se o SSH está ativado:

   ```
   show ip ssh
   ```

   Mostrar exemplo

   ```
   (switch)# show ip ssh

   SSH Configuration

   Administrative Mode: ..... Enabled
   SSH Port: ..... 22
   Protocol Level: ..... Version 2
   SSH Sessions Currently Active: ..... 0
   Max SSH Sessions Allowed: ..... 5
   SSH Timeout (mins): ..... 5
   Keys Present: ..... DSA(1024) RSA(1024)
   ECDSA(521)
   Key Generation In Progress: ..... None
   SSH Public Key Authentication Mode: ..... Enabled
   SCP server Administrative Mode: ..... Enabled
   ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Redefinir o switch de cluster BES-53248 para os padrões de fábrica

Para redefinir o switch de cluster BES-53248 para os padrões de fábrica, você deve apagar as configurações do switch BES-53248.

Sobre esta tarefa

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

Passos

1. Mude para o prompt de comando elevado.

   ```
   (cs2)> enable
   (cs2)#
   ```

2. Apague a configuração de inicialização.

   ```
   erase startup-config
   ```

```
(cs2)# erase startup-config

Are you sure you want to clear the configuration? (y/n) y
```

3. Reinicie o switch.

```
(cs2)# 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**.

1. Aguarde até que o switch seja recarregado e, em seguida, faça login nele.

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

```
(Routing)>
```

Atualize o switch

Fluxo de trabalho de atualização para switches de cluster BES-53248

Siga estas etapas para atualizar o software EFOS e os arquivos de configuração de referência (RCFs) em switches de cluster Broadcom BES-54328, conforme aplicável.

1. **"Atualize sua versão EFOS"**

Faça o download e instale o software do sistema operacional de malha Ethernet (EFOS) no switch de cluster BES-53248.

2. **"Atualize sua versão RCF"**

Atualize o RCF no switch de cluster BES-53248 e verifique as portas para obter uma licença adicional depois que o RCF for aplicado.

3. **"Verifique a rede do cluster ONTAP após a atualização"**

Verifique a integridade da rede do cluster ONTAP após uma atualização do software EFOS ou RCF para switches de cluster BES-53248.

Atualize o software EFOS

Siga estes passos para atualizar o software EFOS no switch de cluster BES-53248.

O software EFOS inclui um conjunto de funcionalidades de rede avançadas e protocolos para o desenvolvimento de sistemas de infra-estrutura Ethernet e IP. Esta arquitetura de software é adequada para qualquer dispositivo organizacional de rede usando aplicativos que exigem inspeção ou separação de pacotes minuciosa.

Prepare-se para a atualização

Antes de começar

- Faça o download do software Broadcom EFOS aplicável para seus switches de cluster a partir "Suporte ao comutador Ethernet Broadcom" do site.
- Reveja as seguintes notas sobre as versões do EFOS.

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.

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	Atualize a nova imagem EFOS usando Método 1: Atualizar o EFOSo . 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 Método 1: Atualizar o EFOSusando o . 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 Método 1: Atualizar o EFOS. 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	
Atualize a nova imagem EFOS usando Método 1: Atualizar o EFOSo . 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	Atualize a nova imagem EFOS usando Método 1: Atualizar o EFOSo . 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	Atualização da imagem EFOS usando Método 2: Atualizar o EFOS usando a instalação do sistema operacional ONIEo . A configuração do switch e as informações da licença serão perdidas.

Para verificar se sua versão do EFOS é compatível com FIPS ou não compatível com FIPS, use o `show fips status` comando. Nos exemplos a seguir, **IP_switch_A1** está usando EFOS compatível com FIPS e **IP_switch_A2** está usando EFOS não compatível com FIPS.

- Switch IP_switch_A1 (EFOS compatível com FIPS):

```
IP_switch_a1 # show fips status

System running in FIPS mode
```

- Switch IP_switch_A2 (EFOS não compatível com FIPS):

```
IP_switch_a2 # show fips status
                        ^
% Invalid input detected at ^ marker.
```

Atualize o software

Use um dos seguintes métodos:

- Método 1: Atualizar o EFOS. Use para a maioria dos casos (consulte a tabela acima).
- Método 2: Atualizar o EFOS usando a instalação do sistema operacional ONIE. Use se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS.

Atualize o EFOS em um switch de cada vez para garantir a operação contínua da rede de cluster.

Método 1: Atualizar o EFOS

Execute os seguintes passos para atualizar o software EFOS.

Observe que depois de atualizar os switches de cluster BES-53248 do EFOS 3,3.x.x ou 3,4.x.x para o EFOS 3.7.0.4 ou 3,8.0,2, os ISLs (Inter-Switch Links) e os canais de porta estão marcados no estado **para baixo**. Este é o comportamento esperado e é seguro continuar com a atualização, a menos que você esteja tendo problemas com LIFs de reversão automática. Consulte o artigo da base de dados de Conhecimento: "Falha na atualização do NDU do comutador de cluster BES-53248 para o EFOS 3.7.0.4 e posterior" Para obter mais detalhes.

Passos

1. Conete o switch de cluster BES-53248 à rede de gerenciamento.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda EFOS, licenças e o arquivo RCF.

   Este exemplo verifica se o switch está conetado ao servidor no endereço IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Desative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

4. Apresentar as imagens de arranque para a configuração ativa e de cópia de segurança:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# show bootvar

 Image Descriptions

 active :
 backup :

 Images currently available on Flash
--------------------------------------------------------------------
 unit      active      backup        current-active    next-active
--------------------------------------------------------------------
    1      3.7.0.4     3.4.4.6             3.7.0.4        3.7.0.4
```

5. Transfira o ficheiro de imagem para o interrutor.

   Copiar o arquivo de imagem para a imagem de backup significa que, quando você reinicializar, essa imagem estabelecerá a versão do EFOS em execução, concluindo a atualização.

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk backup
Remote Password:**

Mode..................................... SFTP
Set Server IP.............................. 172.19.2.1
Path....................................... //tmp/
Filename................................... EFOS-3.10.0.3.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
SFTP Code transfer starting...


File transfer operation completed successfully.
```

6. Apresentar as imagens de arranque para a configuração ativa e de cópia de segurança:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# 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       3.10.0.3
```

7. Inicie o sistema a partir da configuração de cópia de segurança:

   `boot system backup`

```
(cs2)# boot system backup
Activating image backup ..
```

8. Apresentar as imagens de arranque para a configuração ativa e de cópia de segurança:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# show bootvar

Image Descriptions

 active :
 backup :

 Images currently available on Flash
--------------------------------------------------------------------
 unit      active      backup      current-active    next-active
--------------------------------------------------------------------
    1    3.10.0.3    3.10.0.3            3.10.0.3       3.10.0.3
```

9. Salve a configuração em execução na configuração de inicialização:

   `write memory`

   Mostrar exemplo

```
(cs2)# 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!
```

10. Reinicie o switch:

    `reload`

Mostrar exemplo

```
(cs2)# reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

11. Inicie sessão novamente e verifique a nova versão do software EFOS:

`show version`

Mostrar exemplo

```
(cs2)# show version

Switch: 1

System Description..............................  BES-53248A1,
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04
Machine Type....................................  BES-53248A1,
Machine Model...................................  BES-53248
Serial Number...................................  QTFCU38260023
Maintenance Level...............................  A
Manufacturer....................................  0xbc00
Burned In MAC Address...........................  D8:C4:97:71:0F:40
Software Version................................  3.10.0.3
Operating System................................  Linux 4.4.211-
28a6fe76
Network Processing Device.......................  BCM56873_A0
CPLD Version....................................  0xff040c03

Additional Packages.............................  BGP-4
.............................................  QOS
.............................................  Multicast
.............................................  IPv6
.............................................  Routing
.............................................  Data Center
.............................................  OpEN API
.............................................  Prototype Open API
```

12. Repita os passos 5 a 11 no interrutor CS1.
13. Ative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

14. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role Cluster
```

Para obter mais detalhes, "Reverter um LIF para sua porta inicial"consulte .

Método 2: Atualizar o EFOS usando a instalação do sistema operacional ONIE

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 atualizar a imagem EFOS 3,7.x.x não compatível com FIPS ou FIPS do ONIE se o switch não inicializar.

Esta funcionalidade só está disponível para EFOS 3,7.x.x ou posterior não compatível com FIPS.

Se você atualizar o EFOS usando a instalação do ONIE os, a configuração será redefinida para os padrões de fábrica e as licenças serão excluídas. Você deve configurar o switch e instalar licenças e um RCF suportado para retornar o switch à operação normal.

Passos

1. Desative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

2. Inicialize o switch no modo de instalação ONIE.

Durante o arranque, selecione ONIE quando vir o aviso:

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

Depois de selecionar **ONIE**, o switch carrega e apresenta várias opções. Selecione **Instalar os**.

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

O switch inicializa no modo de instalação ONIE.

3. 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 continua e as mensagens são impressas no console.

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

4. 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
```

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

   `ping`

   Mostrar exemplo

```
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:/ #
```

6. Instale o novo software do interrutor:

   `ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86_64`

Mostrar exemplo

```
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 instala e, em seguida, reinicia o interrutor. Deixe o switch reiniciar normalmente para a nova versão do EFOS.

7. Verifique se o novo software do switch está instalado:

   `show bootvar`

   Mostrar exemplo

```
(cs2)# 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         3.10.0.3
(cs2) #
```

8. Conclua a instalação. O switch reinicializa sem nenhuma configuração aplicada e redefine para os padrões de fábrica. Execute as seguintes etapas para reconfigurar o switch:
   a. "Instalar licenças"
   b. "Instale o RCF"
   c. "Ativar SSH"
   d. "Ativar a coleção de registos"

e. "Configure o SNMPv3 para monitoramento"

9. Repita os passos 2 a 8 no interrutor CS1.
10. Ative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

11. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role Cluster
```

Para obter mais detalhes, "Reverter um LIF para sua porta inicial"consulte .

Atualizar o ficheiro de configuração de referência (RCF)

Você pode atualizar o RCF (Reference Configuration File) após atualizar o EFOS do switch de cluster BES-53248 e depois de aplicar novas licenças.

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O arquivo RCF atual, disponível na "Switches de cluster Broadcom" página.
- Uma configuração de inicialização no RCF que reflete as imagens de inicialização desejadas, necessária se você estiver instalando apenas o EFOS e mantendo sua versão atual do RCF. Se você precisar alterar a configuração de inicialização para refletir as imagens de inicialização atuais, você deve fazê-lo antes de reaplicar o RCF para que a versão correta seja instanciada em futuras reinicializações.
- Uma conexão de console ao switch, necessária ao instalar o RCF a partir de um estado padrão de fábrica. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota"para limpar a configuração de antemão.

Documentação sugerida

- Consulte a tabela de compatibilidade do switch para as versões ONTAP e RCF suportadas. Consulte a "Baixar o software EFOS" página. Note que pode haver dependências de comando entre a sintaxe de comando no RCF e aquela encontrada em versões do EFOS.
- Consulte os guias de software e atualização apropriados disponíveis no "Broadcom" site para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch BES-53248.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches BES-53248 são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-

03_clus1, cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.

- O `cluster1::*>` prompt indica o nome do cluster.
- Os exemplos neste procedimento usam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE `e0a` e `e0b`. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Broadcom switch; os comandos ONTAP são usados, a menos que indicado de outra forma.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Antes de instalar uma nova versão de software de switch e RCFs, use o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" . Se você precisar apagar completamente as configurações do switch, então você precisará executar a configuração básica novamente. Você deve estar conetado ao switch usando o console serial, já que uma eliminação completa da configuração redefine a configuração da rede de gerenciamento.

Passo 1: Prepare-se para a atualização

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde *x* é a duração da janela de manutenção em horas.

   A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   system node autosupport invoke -node * -type all -message MAINT=2h
   ```

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
cluster1-02/cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
cluster1-03/cdp
            e0a    cs1                       0/4               BES-
53248
            e0b    cs2                       0/4               BES-
53248
cluster1-04/cdp
            e0a    cs1                       0/3               BES-
53248
            e0b    cs2                       0/3               BES-
53248
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0b     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0b     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
```

5. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. Desativar reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Etapa 2: Configurar portas

1. No switch CS2, confirme a lista de portas que estão conetadas aos nós no cluster.

```
show isdp neighbor
```

2. No switch CS2, encerre as portas conetadas às portas do cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conetadas a nós ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

3. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

4. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se você ainda não fez isso, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração no interrutor CS2 e execute uma configuração básica.

Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado ao switch usando o console serial para apagar as configurações do switch. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Broadcom, mantendo a conetividade remota" para limpar a configuração de antemão.

Limpar a configuração não exclui licenças.

a. SSH para o switch.

Só prossiga quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para que a configuração seja apagada.

b. Entrar no modo de privilégio:

```
(cs2)> enable
(cs2)#
```

c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior usada, alguns comandos podem gerar um erro se uma configuração específica não estiver presente):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```

```
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDstA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
show running-config
```

d. Salve a configuração em execução na configuração de inicialização:

```
write memory
```

```
(cs2)# 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!
```

e. Execute uma reinicialização do switch:

```
reload
```

```
(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
```

a. Faça login no switch novamente usando SSH para concluir a instalação do RCF.

7. Observe o seguinte:
   a. Se tiverem sido instaladas licenças de porta adicionais no switch, você deverá modificar o RCF para configurar as portas licenciadas adicionais. "Ative portas recém-licenciadas"Consulte para obter detalhes.
   b. Grave todas as personalizações que foram feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, definir velocidades de porta ou o modo FEC de codificação forçada.

EFOS versão 3,12.x e posterior

1. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Este exemplo mostra que o SFTP está sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
(cs2)# copy sftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..................................... TFTP
Set Server IP.................................. 172.19.2.1
Path..................................... /
Filename..................................... BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type.................................... Config Script
Destination Filename.......................... reference-config.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifique se o script foi baixado e salvo sob o nome do arquivo que você deu:

   `script list`

```
(cs2)# script list

Configuration Script Name                  Size(Bytes)  Date of
Modification
---------------------------------------  -----------
--------------------
reference-config.scr                       2680         2024 05 31
21:54:22
2 configuration script(s) found.
2042 Kbytes free.
```

2. Aplique o script ao switch:

   `script apply`

```
(cs2)# script apply reference-config.scr

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

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'reference-config.scr' applied.
```

Todas as outras versões do EFOS

1. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Este exemplo mostra que o SFTP está sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt
nvram:script BES-53248_RCF_v1.9-Cluster-HA.scr
Remote Password:**
Mode..................................... SFTP
Set Server IP.............................. 172.19.2.1
Path..................................... //tmp/
Filename................................. BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type................................ Config Script
Destination Filename..................... BES-53248_RCF_v1.9-
Cluster-HA.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifique se o script foi baixado e salvo no nome do arquivo que você deu:

   ```
   script list
   ```

```
(cs2)# script list

Configuration Script Name                    Size(Bytes)  Date of
Modification
-----------------------------------------  -----------
--------------------
BES-53248_RCF_v1.9-Cluster-HA.scr          2241         2020 09 30
05:41:00

1 configuration script(s) found.
```

2. Aplique o script ao switch:

   `script apply`

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.scr

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

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. examine a saída do banner a partir do `show clibanner` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

   `show clibanner`

Mostrar exemplo

```
(cs2)# show clibanner

Banner Message configured :
=========================
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA

Switch   : BES-53248
Filename : BES-53248-RCF-v1.9-Cluster.txt
Date     : 10-26-2022
Version  : v1.9
Port Usage:
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added
right to left
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
NOTE:
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms
of port
speed:
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-
40, 41-44,
45-48
The port speed should be the same (10GbE or 25GbE) across all ports
in a 4-port
group
- If additional licenses are purchased, follow the 'Additional Node
Ports
activated with Licenses' section for instructions
- If SSH is active, it will have to be re-enabled manually after
'erase
startup-config'
command has been executed and the switch rebooted
```

2. No switch, verifique se as portas licenciadas adicionais aparecem depois que o RCF é aplicado:

```
show port all | exclude Detach
```

Mostrar exemplo

```
(cs2)# show port all | exclude Detach

                Admin     Physical     Physical   Link   Link
LACP   Actor
Intf      Type  Mode      Mode         Status     Status Trap
Mode   Timeout
--------- ------ --------- ------------ ---------- ------ -------
------ --------
0/1             Enable    Auto                    Down   Enable
Enable long
0/2             Enable    Auto                    Down   Enable
Enable long
0/3             Enable    Auto                    Down   Enable
Enable long
0/4             Enable    Auto                    Down   Enable
Enable long
0/5             Enable    Auto                    Down   Enable
Enable long
0/6             Enable    Auto                    Down   Enable
Enable long
0/7             Enable    Auto                    Down   Enable
Enable long
0/8             Enable    Auto                    Down   Enable
Enable long
0/9             Enable    Auto                    Down   Enable
Enable long
0/10            Enable    Auto                    Down   Enable
Enable long
0/11            Enable    Auto                    Down   Enable
Enable long
0/12            Enable    Auto                    Down   Enable
Enable long
0/13            Enable    Auto                    Down   Enable
Enable long
0/14            Enable    Auto                    Down   Enable
Enable long
0/15            Enable    Auto                    Down   Enable
Enable long
0/16            Enable    Auto                    Down   Enable
Enable long
0/49            Enable    40G Full                Down   Enable
Enable long
0/50            Enable    40G Full                Down   Enable
Enable long
```

```
0/51            Enable    100G Full               Down   Enable
Enable long
0/52            Enable    100G Full               Down   Enable
Enable long
0/53            Enable    100G Full               Down   Enable
Enable long
0/54            Enable    100G Full               Down   Enable
Enable long
0/55            Enable    100G Full               Down   Enable
Enable long
0/56            Enable    100G Full               Down   Enable
Enable long
```

3. Verifique no switch se suas alterações foram feitas.

```
show running-config
```

4. Salve a configuração em execução para que ela se torne a configuração de inicialização quando você reiniciar o switch:

   `write memory`

   Mostrar exemplo

```
(cs2)# 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!
```

5. Reinicie o switch e verifique se a configuração em execução está correta.

   `reload`

```
(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

6. No switch de cluster CS2, abra as portas conetadas às portas de cluster dos nós.

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Config)# exit
```

7. Salve a configuração em execução na configuração de inicialização:

   `write memory`

   Mostrar exemplo

   ```
   (cs2)# 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!
   ```

8. Verifique as portas no switch CS2:

   ```
   show interfaces status all | exclude Detach
   ```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

9. Verifique a integridade das portas de cluster no cluster.
   a. Verifique se as portas e0b estão ativas e íntegras em todos os nós do cluster:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02


Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Verifique a integridade do switch a partir do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       0/2
BES-53248
            e0b    cs2                       0/2
BES-53248
cluster01-2/cdp
            e0a    cs1                       0/1
BES-53248
            e0b    cs2                       0/1
BES-53248
cluster01-3/cdp
            e0a    cs1                       0/4
BES-53248
            e0b    cs2                       0/4
BES-53248
cluster1-04/cdp
            e0a    cs1                       0/3
BES-53248
            e0b    cs2                       0/2
BES-53248
```

10. Verifique se o cluster exibe informações para ambos os switches do cluster.

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando:

```
system switch ethernet show -is-monitoring-enabled-operational true
```

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                         cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address          Model
----------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.228.143.200   BES-
53248
           Serial Number: QTWCU22510008
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP

cs2                           cluster-network    10.228.143.202   BES-
53248
           Serial Number: QTWCU22510009
            Is Monitored: true
                  Reason: None
        Software Version: 3.10.0.3
          Version Source: CDP/ISDP
cluster1::*>
```

1. repita os passos 1 a 20 no interrutor CS1.
2. Ativar a reversão automática nos LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. . Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role Cluster
```

Para obter mais detalhes, "Reverter um LIF para sua porta inicial"consulte .

Etapa 3: Verifique a configuração

1. No switch CS1, verifique se as portas do switch conetadas às portas do cluster estão **up**:

```
show interfaces status all
```

Mostrar exemplo

```
(cs1)# show interfaces status all | exclude Detach

                                Link    Physical    Physical
Media       Flow
Port       Name                 State   Mode        Status      Type
Control     VLAN
---------  -------------------  ------  ----------  ----------
----------  ----------  ------
.
.
.
0/16       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/17       10/25GbE Node Port   Down    Auto
Inactive    Trunk
0/18       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
0/19       10/25GbE Node Port   Up      25G Full    25G Full
25GBase-SR  Inactive    Trunk
.
.
.
0/50       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/51       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/52       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/53       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/54       40/100GbE Node Port  Down    Auto
Inactive    Trunk
0/55       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
0/56       Cluster   ISL Port   Up      Auto        100G Full
Copper      Inactive    Trunk
```

2. Verifique se o ISL entre os interrutores CS1 e CS2 está funcional:

```
show port-channel 1/1
```

Mostrar exemplo

```
(cs1)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port-channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)
Mbr     Device/       Port      Port
Ports   Timeout       Speed     Active
------- ------------- --------- -------
0/55    actor/long    Auto      True
        partner/long
0/56    actor/long    Auto      True
        partner/long
```

3. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0b     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0a     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0b     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0a     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0a     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
```

4. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------- -------------------
------------------- -------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster01-
02_clus1  none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster01-
02_clus2  none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-02_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
  Local 169.254.1.3 to Remote 169.254.1.6
  Local 169.254.1.3 to Remote 169.254.1.7
  Local 169.254.1.3 to Remote 169.254.3.4
  Local 169.254.1.3 to Remote 169.254.3.5
  Local 169.254.1.3 to Remote 169.254.3.8
  Local 169.254.1.3 to Remote 169.254.3.9
  Local 169.254.1.1 to Remote 169.254.1.6
  Local 169.254.1.1 to Remote 169.254.1.7
  Local 169.254.1.1 to Remote 169.254.3.4
  Local 169.254.1.1 to Remote 169.254.3.5
  Local 169.254.1.1 to Remote 169.254.3.8
  Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

1. Altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Verifique a rede do cluster ONTAP após uma atualização do software EFOS ou RCF dos switches do cluster BES-53248

Você pode usar os seguintes comandos para verificar a integridade da rede de cluster ONTAP após uma atualização do software EFOS ou RCF para switches de cluster BES-53248.

Passos

1. Exiba informações sobre as portas de rede no cluster usando o comando:

```
network port show -ipspace Cluster
```

`Link` tem de ter o valor `up` e `Health Status` tem de ser `healthy`.

Mostrar exemplo

O exemplo a seguir mostra a saída do comando:

```
cluster1::> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port   IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
------ ------------ ---------------- ---- ---- ----------- --------
------
e0a    Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b    Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port   IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----  ------------ ---------------- ---- ---- ----------- --------
------
e0a    Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b    Cluster      Cluster          up   9000  auto/10000 healthy
false
```

2. Para cada LIF, verifique se `Is Home` está `true` e `Status Admin/Oper` está `up` em ambos os nós, usando o comando:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.217.125/16 node1
e0a     true
            node1_clus2  up/up    169.254.205.88/16  node1
e0b     true
            node2_clus1  up/up    169.254.252.125/16 node2
e0a     true
            node2_clus2  up/up    169.254.110.131/16 node2
e0b     true
```

3. Verifique se o `Health Status` de cada nó `true` está usando o comando:

   `cluster show`

Mostrar exemplo

```
cluster1::> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migrar os switches

Migre os switches de cluster CN1610 para os switches de cluster BES-53248

Para migrar os switches de cluster CN1610 em um cluster para switches de cluster BES-53248 compatíveis com Broadcom, revise os requisitos de migração e siga o procedimento de migração.

Os seguintes switches de cluster são suportados:

- CN1610
- BES-53248

Rever os requisitos

Verifique se sua configuração atende aos seguintes requisitos:

- Algumas das portas nos switches BES-53248 estão configuradas para serem executadas em 10GbE.
- A conectividade 10GbE dos nós para os switches de cluster BES-53248 foi planejada, migrada e documentada.
- O cluster está totalmente funcionando (não deve haver erros nos logs ou problemas semelhantes).
- A personalização inicial dos switches BES-53248 está concluída, de modo que:
  - Os switches BES-53248 estão executando a versão mais recente recomendada do software EFOS.
  - Os ficheiros de configuração de referência (RCFs) foram aplicados aos comutadores.
  - Qualquer personalização de site, como DNS, NTP, SMTP, SNMP e SSH, é configurada nos novos switches.

Conexões de nós

Os switches do cluster suportam as seguintes conexões de nós:

- NetApp CN1610: Portas de 0/1 a 0/12 (10GbE)
- BES-53248: Portas 0/1-0/16 (10GbE/25GbE)

> Portas adicionais podem ser ativadas comprando licenças de porta.

Portas ISL

Os interrutores do grupo de instrumentos utilizam as seguintes portas ISL (Inter-Switch Link):

- NetApp CN1610: Portas de 0/13 a 0/16 (10GbE)
- BES-53248: Portas 0/55-0/56 (100GbE)

O "*NetApp Hardware Universe*" contém informações sobre compatibilidade com ONTAP, firmware EFOS suportado e cabeamento para switches de cluster BES-53248.

Cablagem ISL

O cabeamento ISL apropriado é o seguinte:

- * Início: * Para CN1610 a CN1610 (SFP para SFP), quatro cabos de fibra ótica SFP ou cobre de conexão direta.
- **Final:** para BES-53248 a BES-53248 (QSFP28 a QSFP28), dois transcetores óticos QSFP28/fibra ou cabos de conexão direta de cobre.

Migrar os switches

Siga este procedimento para migrar os switches do cluster CN1610 para os switches do cluster BES-53248.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os exemplos usam dois nós, cada um implantando duas portas de interconexão de cluster de 10 GbE: `e0a` E `e0b`.
- As saídas de comando podem variar dependendo de diferentes versões do software ONTAP.
- Os CN1610 interrutores a substituir são `CL1` e `CL2`.
- Os interrutores BES-53248 para substituir os interrutores CN1610 são `cs1` e `cs2`.
- Os nós são `node1` e `node2`.
- O interrutor CL2 é substituído primeiro pelo CS2, seguido pelo CL1 pelo CS1.
- Os switches BES-53248 são pré-carregados com as versões suportadas do Reference Configuration File (RCF) e do Ethernet Fabric os (EFOS) com cabos ISL ligados nas portas 55 e 56.
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O cluster começa com dois nós conetados a dois switches de cluster CN1610.
- O interrutor CN1610 CL2 é substituído pelo interrutor BES-53248 CS2:
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - Desconete os cabos de todas as portas do cluster em todos os nós conetados ao CL2 e, em seguida, use os cabos suportados para reconetar as portas ao novo switch de cluster CS2.
- O interrutor CN1610 CL1 é substituído pelo interrutor BES-53248 CS1:
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - Desconete os cabos de todas as portas do cluster em todos os nós conetados ao CL1 e, em seguida, use os cabos suportados para reconetar as portas ao novo switch de cluster CS1.

> Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

onde x é a duração da janela de manutenção em horas.

> A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

O seguinte comando suprime a criação automática de casos por duas horas:

```
cluster1::*> system node autosupport invoke -node * -type all -message
MAINT=2h
```

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

Etapa 2: Configurar portas e cabeamento

1. Nos novos switches, confirme se o ISL está cabeado e funcionando corretamente entre os switches CS1 e CS2:

   ```
   show port-channel
   ```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL são **up** no switch CS1:

```
(cs1)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

O exemplo a seguir mostra que as portas ISL são **up** no switch CS2:

```
(cs2)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

2. Exiba as portas de cluster em cada nó conetado aos switches de cluster existentes:

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

O exemplo a seguir mostra quantas interfaces de interconexão de cluster foram configuradas em cada nó para cada switch de interconexão de cluster:

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    CL1                       0/2
CN1610
            e0b    CL2                       0/2
CN1610
node1      /cdp
            e0a    CL1                       0/1
CN1610
            e0b    CL2                       0/1
CN1610
```

3. Determine o status administrativo ou operacional de cada interface de cluster.

   a. Verifique se todas as portas do cluster estão `up` com `healthy` um status:

      ```
      network port show -ipspace Cluster
      ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

b. Verifique se todas as interfaces de cluster (LIFs) estão em suas portas iniciais:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
```

4. Verifique se o cluster exibe informações para ambos os switches do cluster:

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando: `system switch ethernet show -is-monitoring-enabled-operational true`

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                        Type              Address       Model
----------------------------- ----------------- ------------- --------
CL1                           cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP

CL2                           cluster-network  10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP
cluster1::*>
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando: `system cluster-switch show -is-monitoring-enabled-operational true`

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type              Address       Model
----------------------------- ----------------- ------------- --------
CL1                           cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP

CL2                           cluster-network  10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP
cluster1::*>
```

1. Desativar reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

2. No switch de cluster CL2, encerre as portas conetadas às portas de cluster dos nós para fazer failover das LIFs de cluster:

```
(CL2)# configure
(CL2)(Config)# interface 0/1-0/16
(CL2)(Interface 0/1-0/16)# shutdown
(CL2)(Interface 0/1-0/16)# exit
(CL2)(Config)# exit
(CL2)#
```

3. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch de cluster CL1. Isso pode levar alguns segundos.

   ```
   network interface show -vserver Cluster
   ```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0a     false
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false
```

4. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

5. Mova todos os cabos de conexão do nó do cluster do antigo switch CL2 para o novo switch CS2.
6. Confirme a integridade das conexões de rede movidas para CS2:

   `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Todas as portas de cluster que foram movidas devem ser `up`.

7. Verifique as informações do vizinho nas portas do cluster:

   `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    CL1                       0/2
CN1610
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    CL1                       0/1
CN1610
            e0b    cs2                       0/1               BES-
53248
```

8. Confirme se as conexões da porta do switch estão em bom estado do ponto de vista do switch CS2:

```
cs2# show interface all
cs2# show isdp neighbors
```

9. No switch de cluster CL1, encerre as portas conetadas às portas de cluster dos nós para fazer failover das LIFs de cluster:

```
(CL1)# configure
(CL1)(Config)# interface 0/1-0/16
(CL1)(Interface 0/1-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

Todos os LIFs de cluster fazem failover para o switch CS2.

10. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch CS2. Isso pode levar alguns segundos:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0b     false
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0b     false
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

11. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

    ```
    cluster1::*> cluster show
    Node       Health  Eligibility   Epsilon
    ---------- ------- ------------- -------
    node1      true    true          false
    node2      true    true          false
    ```

12. Mova os cabos de conexão do nó do cluster de CL1 para o novo switch CS1.
13. Confirme a integridade das conexões de rede movidas para CS1:

    `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Todas as portas de cluster que foram movidas devem ser `up`.

14. Verifique as informações do vizinho nas portas do cluster:

    `network device-discovery show`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
```

15. Confirme se as conexões da porta do switch estão em bom estado do ponto de vista do switch CS1:

```
cs1# show interface all
cs1# show isdp neighbors
```

16. Verifique se o ISL entre CS1 e CS2 ainda está operacional:

```
show port-channel
```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL são **up** no switch CS1:

```
(cs1)# show port-channel 1/1
Local Interface............................... 1/1
Channel Name.................................. Cluster-ISL
Link State.................................... Up
Admin Mode.................................... Enabled
Type.......................................... Dynamic
Port channel Min-links........................ 1
Load Balance Option........................... 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

O exemplo a seguir mostra que as portas ISL são **up** no switch CS2:

```
(cs2)# show port-channel 1/1
Local Interface............................... 1/1
Channel Name.................................. Cluster-ISL
Link State.................................... Up
Admin Mode.................................... Enabled
Type.......................................... Dynamic
Port channel Min-links........................ 1
Load Balance Option........................... 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

17. Exclua os switches CN1610 substituídos da tabela de switches do cluster, se eles não forem removidos

automaticamente:

ONTAP 9 F.8 e mais tarde

A partir de ONTAP 9.8, use o comando: `system switch ethernet delete -device *device-name*`

```
cluster::*> system switch ethernet delete -device CL1
cluster::*> system switch ethernet delete -device CL2
```

ONTAP 9 F.7 e anteriores

Para o ONTAP 9.7 e versões anteriores, use o comando: `system cluster-switch delete -device *device-name*`

```
cluster::*> system cluster-switch delete -device CL1
cluster::*> system cluster-switch delete -device CL2
```

Etapa 3: Verifique a configuração

1. Ative a reversão automática nos LIFs do cluster.

   ```
   cluster1::*> network interface modify -vserver Cluster -lif * -auto
   -revert true
   ```

2. Verifique se os LIFs de cluster reverteram para suas portas residenciais (isso pode levar um minuto):

   ```
   network interface show -vserver Cluster
   ```

   Se os LIFs de cluster não tiverem revertido para sua porta inicial, reverta-os manualmente:

   ```
   network interface revert -vserver Cluster -lif *
   ```

3. Verifique se o cluster está em bom estado:

   ```
   cluster show
   ```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

```
cluster::*> system node autosupport invoke -node * -type all -message
MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migrar para um ambiente de cluster comutado do NetApp

Se você tiver um ambiente de cluster *sem switch* de dois nós existente, poderá migrar para um ambiente de cluster *comutado* de dois nós usando switches de cluster BES-53248 compatíveis com Broadcom, o que permite que você escale além de dois nós no cluster.

O processo de migração funciona para todas as portas de nós de cluster que usam portas óticas ou Twinax, mas não é suportado neste switch se os nós estiverem usando portas 10GBASEBASE-T RJ45 integradas para as portas de rede do cluster.

Rever os requisitos

Revise os requisitos a seguir para o ambiente de cluster.

- Esteja ciente de que a maioria dos sistemas requer duas portas de rede de cluster dedicadas em cada controlador.
- Certifique-se de que o switch de cluster BES-53248 está configurado como descrito em "Substitua os requisitos" antes de iniciar este processo de migração.
- Para a configuração sem switch de dois nós, certifique-se de que:
  - A configuração sem switch de dois nós está corretamente configurada e funcionando.
  - Os nós estão executando o ONTAP 9.5P8 e posterior. O suporte para portas de cluster de 40/100 GbE começa com o firmware EFOS versão 3.4.4.6 e posterior.
  - Todas as portas de cluster estão no estado **up**.
  - Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e em suas portas domésticas.
- Para a configuração do switch de cluster BES-53248 compatível com Broadcom, certifique-se de que:
  - O comutador de cluster BES-53248 está totalmente funcional em ambos os interrutores.
  - Ambos os switches têm conetividade de rede de gerenciamento.
  - Existe acesso à consola aos interrutores do cluster.
  - As conexões de switch nó a nó BES-53248 e switch a switch estão usando cabos Twinax ou fibra.

    O "*NetApp Hardware Universe*" contém informações sobre compatibilidade com ONTAP, firmware EFOS suportado e cabeamento para switches BES-53248.
- Os cabos ISL (Inter-Switch Link) são conetados às portas 0/55 e 0/56 em ambos os switches BES-53248.
- A personalização inicial de ambos os switches BES-53248 está concluída, de modo que:
  - Os switches BES-53248 estão executando a versão mais recente do software.
  - Os switches BES-53248 têm licenças de porta opcionais instaladas, se compradas.
  - Os arquivos de configuração de referência (RCFs) são aplicados aos switches.
- Qualquer personalização de site (SMTP, SNMP e SSH) é configurada nos novos switches.

Restrições de velocidade do grupo de portas

- As portas 48 10/25GbE (SFP28/SFP) são combinadas em 12 grupos de 4 portas da seguinte forma: Portas 1-33, 36-32, 28-29, 25-21, 24-20, 16-17, 13-9, 12-8, 4-5, 37-40, 41-44 e 45-48.
- A velocidade da porta SFP28/SFP deve ser a mesma (10GbE ou 25GbE) em todas as portas do grupo de 4 portas.
- Se as velocidades em um grupo de 4 portas forem diferentes, as portas do switch não funcionarão corretamente.

Migrar para o ambiente de cluster

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches BES-53248 são `cs1` e `cs2`.
- Os nomes dos SVMs do cluster são `node1` e `node2`.

- Os nomes dos LIFs são `node1_clus1` e `node1_clus2` no nó 1 e `node2_clus1` e `node2_clus2` no nó 2, respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas do cluster usadas neste procedimento são `e0a` e `e0b`.

  O "*NetApp Hardware Universe*" contém as informações mais recentes sobre as portas de cluster reais para as suas plataformas.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   cluster1::*> system node autosupport invoke -node * -type all -message
   MAINT=2h
   ```

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   `set -privilege advanced`

   (`*>`É apresentado o aviso avançado).

Etapa 2: Configurar portas e cabeamento

1. Desative todas as portas ativadas voltadas para o nó (não portas ISL) nos novos switches de cluster CS1 **e** CS2.

   > Não deve desativar as portas ISL.

   O exemplo a seguir mostra que as portas 1 a 16 voltadas para o nó estão desativadas no switch CS1:

   ```
   (cs1)# configure
   (cs1)(Config)# interface 0/1-0/16
   (cs1)(Interface 0/1-0/16)# shutdown
   (cs1)(Interface 0/1-0/16)# exit
   (cs1)(Config)# exit
   ```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches BES-53248 CS1 e CS2 estão ativos:

```
show port-channel
```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS1:

```
(cs1)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS2:

```
(cs2)# show port-channel 1/1
Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------  -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

3. Exibir a lista de dispositivos vizinhos:

```
show isdp neighbors
```

Este comando fornece informações sobre os dispositivos que estão conetados ao sistema.

Mostrar exemplo

O exemplo a seguir lista os dispositivos vizinhos no switch CS1:

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf     Holdtime  Capability   Platform    Port ID
-------------- -------- --------- ------------ ----------- ---------
cs2            0/55     176       R            BES-53248   0/55
cs2            0/56     176       R            BES-53248   0/56
```

O exemplo a seguir lista os dispositivos vizinhos no switch CS2:

```
(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf     Holdtime  Capability   Platform    Port ID
-------------- -------- --------- ------------ ----------- ---------
cs2            0/55     176       R            BES-53248   0/55
cs2            0/56     176       R            BES-53248   0/56
```

4. Verifique se todas as portas do cluster estão ativas:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

                                                            Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node2

                                                            Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy
```

5. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

6. Desative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

7. Desconete o cabo da porta de cluster e0a no node1 e conete o e0a à porta 1 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches BES-53248.

   O "*NetApp Hardware Universe*" contém mais informações sobre cabeamento.

8. Desconete o cabo da porta de cluster e0a no node2 e conete o e0a à porta 2 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches BES-53248.
9. Habilite todas as portas voltadas para o nó no switch de cluster CS1.

   O exemplo a seguir mostra que as portas 1 a 16 estão ativadas no switch CS1:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# no shutdown
(cs1)(Interface 0/1-0/16)# exit
(cs1)(Config)# exit
```

10. Verifique se todas as portas do cluster estão ativas:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

11. Verifique se todas as LIFs de cluster estão ativas e operacionais:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node        Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1       e0a
false
         node1_clus2  up/up      169.254.49.125/16  node1       e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2       e0a
false
         node2_clus2  up/up      169.254.19.183/16  node2       e0b
true
```

12. Exibir informações sobre o status dos nós no cluster:

    `cluster show`

    Mostrar exemplo

    O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

    ```
    cluster1::*> cluster show

    Node                 Health  Eligibility   Epsilon
    -------------------- ------- ------------  ------------
    node1                true    true          false
    node2                true    true          false
    ```

13. Desconete o cabo da porta de cluster e0b no node1 e conete o e0b à porta 1 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches BES-53248.
14. Desconete o cabo da porta de cluster e0b no node2 e conete o e0b à porta 2 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches BES-53248.
15. Habilite todas as portas voltadas para o nó no switch de cluster CS2.

    O exemplo a seguir mostra que as portas 1 a 16 estão ativadas no switch CS2:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)# exit
```

16. Verifique se todas as portas do cluster estão ativas:

`network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Etapa 3: Verifique a configuração

1. Ative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert true
```

2. Verifique se os LIFs de cluster reverteram para suas portas residenciais (isso pode levar um minuto):

   `network interface show -vserver Cluster`

   Se os LIFs de cluster não tiverem revertido para sua porta inicial, reverta-os manualmente:

   `network interface revert -vserver Cluster -lif *`

3. Verifique se todas as interfaces são exibidas `true` para `Is Home`:

   `network interface show -vserver Cluster`

   Isso pode levar vários minutos para ser concluído.

   Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true
```

4. Verifique se ambos os nós têm uma conexão com cada switch:

   `show isdp neighbors`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf         Holdtime  Capability   Platform -- Port
ID
-------------- ------------ --------- ------------ -----------
----------
node1          0/1          175       H            FAS2750     e0a
node2          0/2          157       H            FAS2750     e0a
cs2            0/55         178       R            BES-53248   0/55
cs2            0/56         178       R            BES-53248   0/56


(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf         Holdtime  Capability   Platform    Port
ID
-------------- ------------ --------- ------------ -----------
------------
node1          0/1          137       H            FAS2750     e0b
node2          0/2          179       H            FAS2750     e0b
cs1            0/55         175       R            BES-53248   0/55
cs1            0/56         175       R            BES-53248   0/56
```

5. Exiba informações sobre os dispositivos de rede descobertos no cluster:

   `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
```

6. Verifique se as definições estão desativadas:

   `network options switchless-cluster show`

   > Pode demorar vários minutos para o comando ser concluído. Aguarde até que o anúncio "3 minutos de duração expire".

   A `false` saída no exemplo a seguir mostra que as configurações estão desativadas:

   ```
   cluster1::*> network options switchless-cluster show
   Enable Switchless Cluster: false
   ```

7. Verifique o status dos membros do nó no cluster:

   `cluster show`

Mostrar exemplo

O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

8. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Mostrar exemplo

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

   Para obter mais informações, consulte: "Artigo da KB do NetApp: Como suprimir a criação automática de casos durante janelas de manutenção programada"

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os interruptores

Requisitos de substituição

Antes de substituir o interrutor, certifique-se de que estão reunidas as seguintes condições no ambiente atual e no interrutor de substituição.

Infraestrutura de cluster e rede existentes

Certifique-se de que:

- O cluster existente é verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
- Todas as portas de cluster são **up**.
- Todas as interfaces lógicas de cluster (LIFs) são administrativamente e operacionalmente **up** e em suas portas domésticas.
- O comando ONTAP `cluster ping-cluster -node node1` deve indicar que as configurações, `basic connectivity` e `larger than PMTU communication`, são bem-sucedidas em todos os caminhos.

Interrutor do cluster de substituição BES-53248

Certifique-se de que:

- A conetividade de rede de gerenciamento no switch de substituição está funcional.
- O acesso do console ao interrutor de substituição está no lugar.
- As conexões de nó são as portas 0/1 a 0/16 com licenciamento padrão.
- Todas as portas ISL (Inter-Switch Link) estão desativadas nas portas 0/55 e 0/56.
- O ficheiro de configuração de referência (RCF) pretendido e a imagem do interrutor do sistema operativo EFOS são carregados no interrutor.
- A personalização inicial do interrutor está completa, como detalhado em "Configure o switch do cluster BES-53248".

Quaisquer personalizações de sites anteriores, como STP, SNMP e SSH, são copiadas para o novo switch.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desativar a criação de casos durante a manutenção. Consulte este artigo da base de dados de Conhecimento "SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para obter mais detalhes.
- Ativar o registo de sessão para quaisquer sessões CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" neste artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Para mais informações

- "Site de suporte da NetApp"
- "NetApp Hardware Universe"

Substitua um switch de cluster BES-53248 compatível com Broadcom

Siga estas etapas para substituir um switch de cluster BES-53248 compatível com Broadcom defeituoso em uma rede de cluster. Este é um procedimento sem interrupções (NDU).

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches BES-53248 existentes são `cs1` e `cs2`.
- O nome do novo switch BES-53248 é `newcs2`.
- Os nomes dos nós são `node1` e `node2`.
- As portas de cluster em cada nó são nomeadas e `e0a` `e0b`.
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.
- O prompt para alterações em todos os nós de cluster é `cluster1::>`

Sobre a topologia

Este procedimento baseia-se na seguinte topologia de rede de cluster:

Mostrar exemplo de topologia

```
cluster1::> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false


Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false


cluster1::> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
true
```

```
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true


cluster1::> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
```

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID                Intf      Holdtime  Capability Platform
Port ID
------------------------ --------- --------- ----------
---------------- ---------
node1                    0/1       175       H          FAS2750
e0a
node2                    0/2       152       H          FAS2750
e0a
cs2                      0/55      179       R          BES-53248
0/55
cs2                      0/56      179       R          BES-53248
0/56


(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID                Intf      Holdtime  Capability Platform
Port ID
------------------------ --------- --------- ----------
---------------- ---------
node1                    0/1       129       H          FAS2750
e0b
node2                    0/2       165       H          FAS2750
e0b
cs1                      0/55      179       R          BES-53248
0/55
cs1                      0/56      179       R          BES-53248
0/56
```

Passos

1. Reveja o "Requisitos de substituição".
2. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

onde *x* é a duração da janela de manutenção em horas.

> A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

3. Instale o ficheiro de configuração de referência (RCF) e a imagem apropriados no switch, newcs2, e faça os preparativos necessários para o local.

   Se necessário, verifique, baixe e instale as versões apropriadas do software RCF e EFOS para o novo switch. Se tiver verificado que o novo switch está corretamente configurado e não necessita de atualizações para o software RCF e EFOS, avance para o passo 2.

   a. Você pode baixar o software Broadcom EFOS aplicável para seus switches de cluster a partir "Suporte ao comutador Ethernet Broadcom" do site. Siga os passos na página Download para transferir o ficheiro EFOS para a versão do software ONTAP que está a instalar.
   b. O RCF apropriado está disponível na "Switches de cluster Broadcom" página. Siga os passos na página de transferência para transferir o RCF correto para a versão do software ONTAP que está a instalar.

4. No novo switch, faça login como `admin` e desligue todas as portas que serão conetadas às interfaces do cluster de nós (portas 1 a 16).

   > Se você comprou licenças adicionais para portas adicionais, encerre essas portas também.

   Se o switch que você está substituindo não estiver funcional e estiver desativado, as LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

   > Não é necessária nenhuma palavra-passe para entrar `enable` no modo.

   Mostrar exemplo

   ```
   User: admin
   Password:
   (newcs2)> enable
   (newcs2)# config
   (newcs2)(config)# interface 0/1-0/16
   (newcs2)(interface 0/1-0/16)# shutdown
   (newcs2)(interface 0/1-0/16)# exit
   (newcs2)(config)# exit
   (newcs2)#
   ```

5. Verifique se todas as LIFs do cluster `auto-revert` estão ativadas:

   ```
   network interface show -vserver Cluster -fields auto-revert
   ```

Mostrar exemplo de topologia

```
cluster1::> network interface show -vserver Cluster -fields auto-
revert

Logical
Vserver   Interface    Auto-revert
--------- ------------ ------------
Cluster   node1_clus1  true
Cluster   node1_clus2  true
Cluster   node2_clus1  true
Cluster   node2_clus2  true
```

6. Desligue as portas ISL 0/55 e 0/56 no interrutor BES-53248 CS1:

Mostrar exemplo de topologia

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# shutdown
```

7. Remova todos os cabos do switch BES-53248 CS2 e conete-os às mesmas portas do switch BES-53248 newcs2.
8. Abra as portas ISLs 0/55 e 0/56 entre os switches CS1 e newcs2 e verifique o status da operação do canal da porta.

   O estado de ligação para o canal de porta 1/1 deve ser **up** e todas as portas membros devem ser verdadeiras sob o título Port ative.

Mostrar exemplo

Este exemplo ativa as portas ISL 0/55 e 0/56 e apresenta o estado de ligação para o canal de porta 1/1 no interrutor CS1:

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# no shutdown
(cs1)(interface 0/55-0/56)# exit
(cs1)# show port-channel 1/1

Local Interface................................ 1/1
Channel Name................................... Cluster-ISL
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Port-channel Min-links......................... 1
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port       Port
Ports  Timeout       Speed      Active
------ ------------- ---------- -------
0/55   actor/long    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

9. No novo switch newcs2, reative todas as portas conetadas às interfaces do cluster de nós (portas 1 a 16).

Se você comprou licenças adicionais para portas adicionais, encerre essas portas também.

Mostrar exemplo

```
User:admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2)(config)# interface 0/1-0/16
(newcs2)(interface 0/1-0/16)# no shutdown
(newcs2)(interface 0/1-0/16)# exit
(newcs2)(config)# exit
```

10. Verifique se a porta e0b é **up**:

    `network port show -ipspace Cluster`

    Mostrar exemplo

    A saída deve ser semelhante ao seguinte:

```
cluster1::> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/auto   -
false
```

11. No mesmo nó que você usou na etapa anterior, aguarde que o cluster LIF node1_clus2 no node1 reverta automaticamente.

Mostrar exemplo

Neste exemplo, LIF node1_clus2 no node1 é revertido com sucesso se `Is Home` é `true` e a porta é e0b.

O comando a seguir exibe informações sobre os LIFs em ambos os nós. Abrir o primeiro nó é bem-sucedido se `Is Home` for `true` para ambas as interfaces de cluster e eles mostrarem as atribuições de porta corretas, neste `e0a` exemplo e `e0b` no node1.

```
cluster::> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false
```

12. Exibir informações sobre os nós em um cluster:

    `cluster show`

    Mostrar exemplo

    Este exemplo mostra que a integridade do nó `node1` para e `node2` neste cluster é `true`:

    ```
    cluster1::> cluster show
    Node   Health   Eligibility   Epsilon
    ------ -------- ------------  --------
    node1  true     true          true
    node2  true     true          true
    ```

13. Confirme a seguinte configuração de rede de cluster:

    `network port show`

```
network interface show
```

Mostrar exemplo

```
cluster1::> network port show -ipspace Cluster
Node: node1

Ignore
                                        Speed(Mbps)            Health
Health
Port      IPspace     Broadcast Domain Link MTU   Admin/Oper  Status
Status
--------- ----------- ---------------- ---- ----- -----------
-------- ------
e0a       Cluster     Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster     Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                         Speed(Mbps)           Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000 auto/10000
healthy  false


cluster1::> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
```

```
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

14. Verifique se a rede do cluster está em bom estado:

```
show isdp neighbors
```

Mostrar exemplo

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID    Intf    Holdtime    Capability    Platform    Port ID
---------    ----    --------    ----------    --------    --------
node1        0/1     175         H             FAS2750     e0a
node2        0/2     152         H             FAS2750     e0a
newcs2       0/55    179         R             BES-53248   0/55
newcs2       0/56    179         R             BES-53248   0/56

(newcs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Intf    Holdtime    Capability    Platform    Port ID
---------    ----    --------    ----------    --------    --------
node1        0/1     129         H             FAS2750     e0b
node2        0/2     165         H             FAS2750     e0b
cs1          0/55    179         R             BES-53248   0/55
cs1          0/56    179         R             BES-53248   0/56
```

15. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os switches de cluster BES-53248 Broadcom por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois

nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

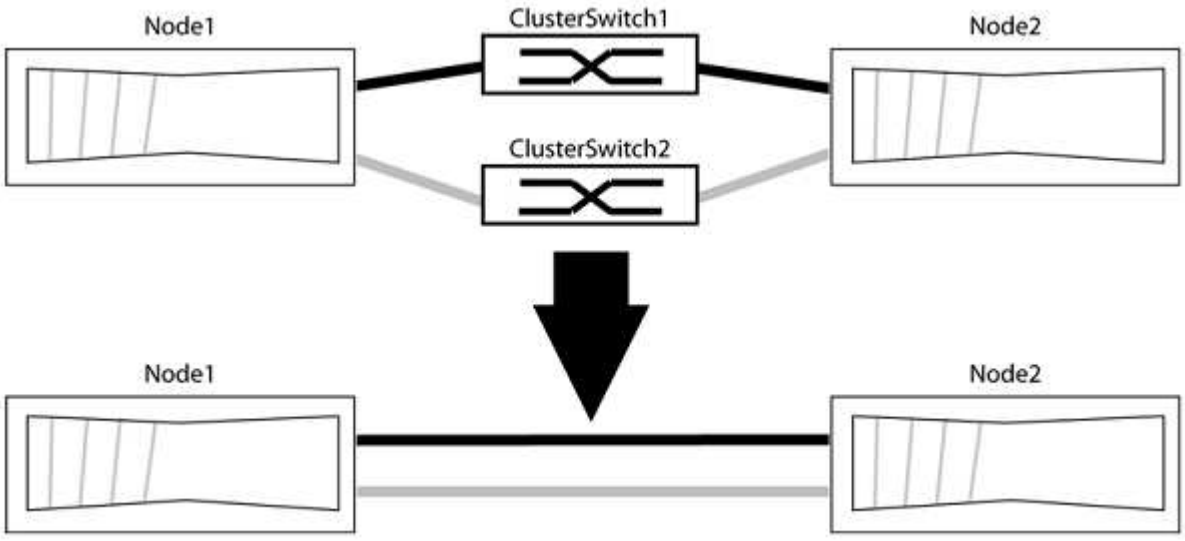
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

   ```
   network options detect-switchless-cluster show
   ```

   Mostrar exemplo

   A saída de exemplo a seguir mostra se a opção está ativada.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message
   MAINT=<number_of_hours>h
   ```

   ```
   `h`onde está a duração da janela de manutenção em horas. A mensagem
   notifica o suporte técnico desta tarefa de manutenção para que possa
   suprimir a criação automática de casos durante a janela de manutenção.
   ```

   No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

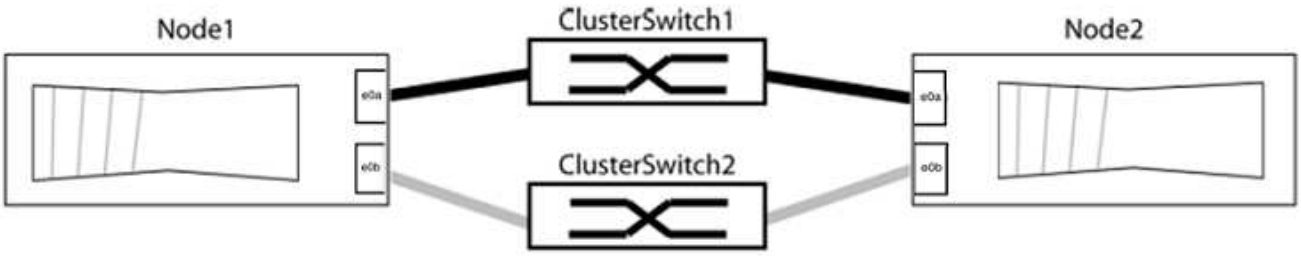
   Mostrar exemplo

   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-bes-53248/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



   Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

   Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

   `network interface show -vserver Cluster -fields is-home`

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

```
network interface revert -vserver Cluster -lif *
```

4. Desativar a reversão automática para as LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

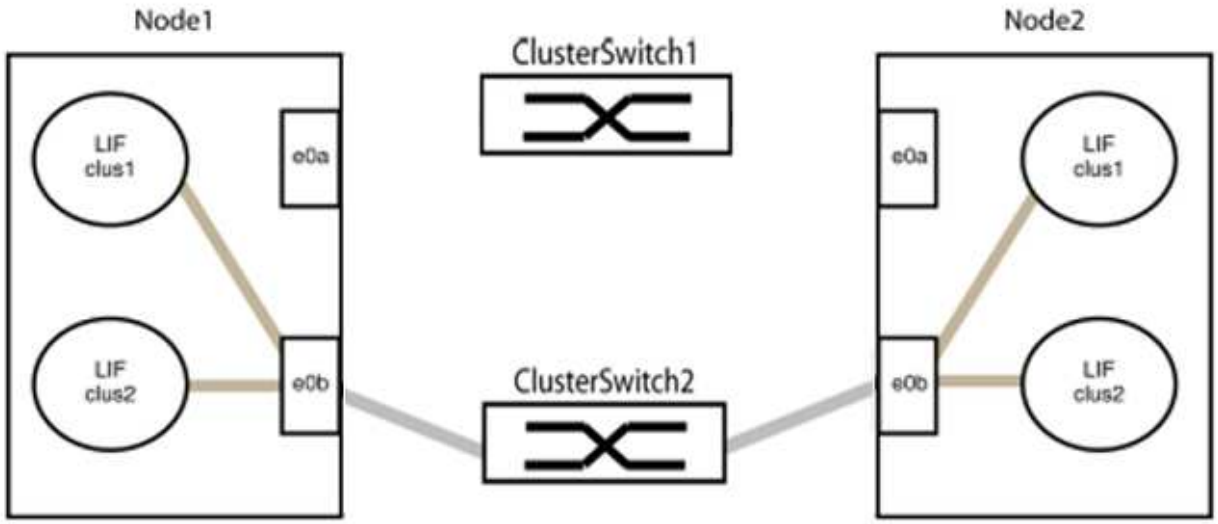
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

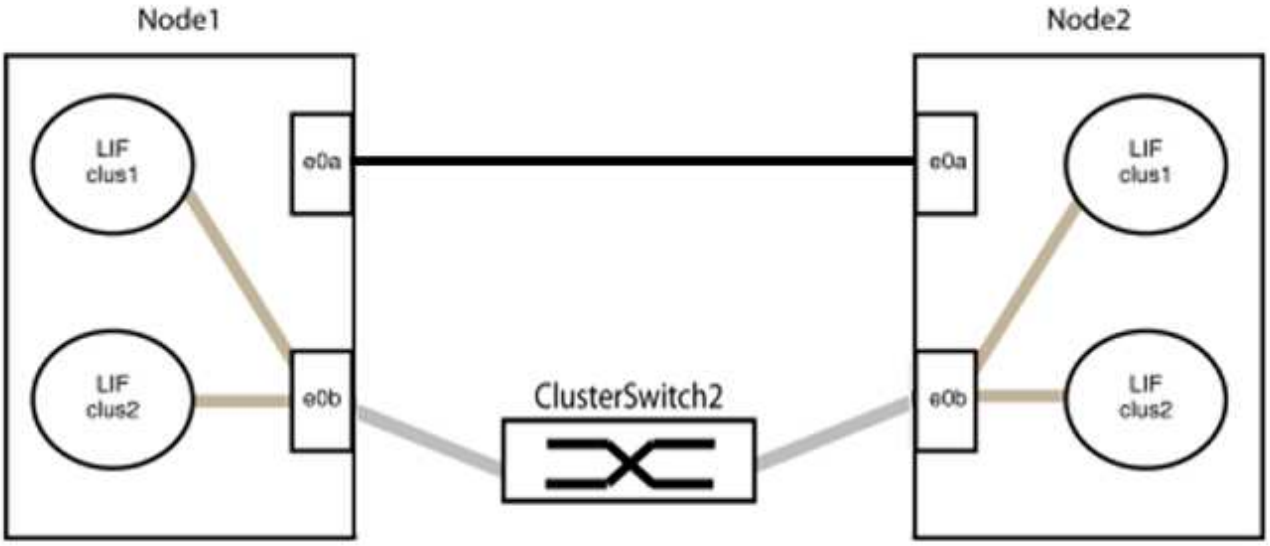
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

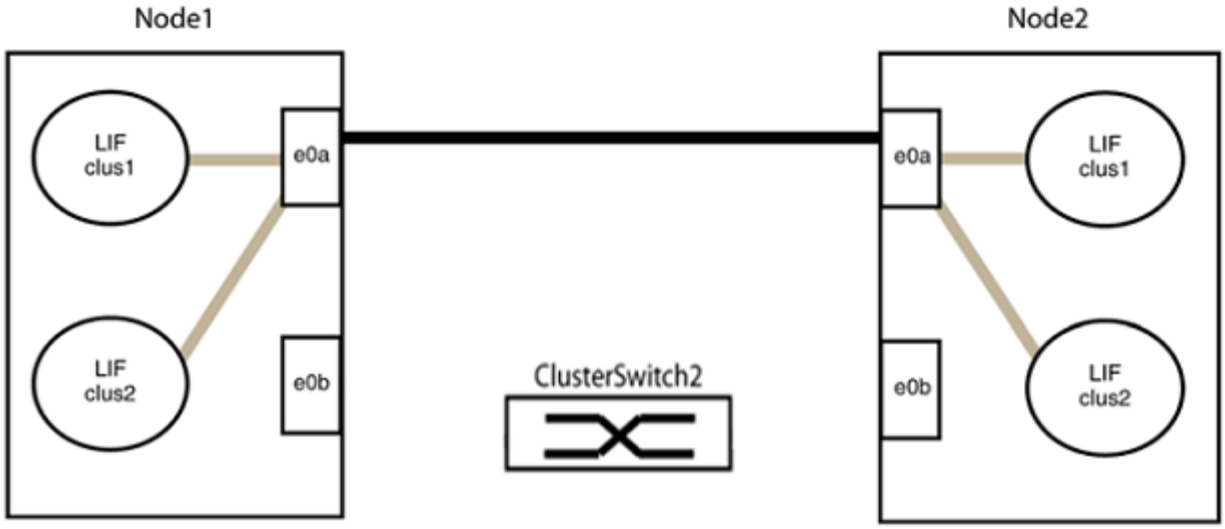
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

Cisco Nexus 9336CP-FX2 ou 9336CP-FX2BASE-T

Comece agora

Fluxo de trabalho de instalação e configuração para switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Os switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T fazem parte da plataforma Cisco Nexus 9000 e podem ser instalados em um gabinete de sistema

NetApp . Os switches de cluster permitem que você crie clusters ONTAP com mais de dois nós.

O Cisco Nexus 9336C-FX2 (36 portas) é um switch de cluster/armazenamento/dados de alta densidade de portas. O Cisco Nexus 9336C-FX2-T (12 portas) é um switch de alto desempenho e baixa densidade de portas que suporta configurações de cluster de 10/25/40/100 GbE.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches Cisco 9336C-FX2 e 9336C-FX2-T.

1. **"Revise os requisitos de configuração"**

Revise os requisitos de configuração para os switches de cluster 9336C-FX2 e 9336C-FX2-T.

2. **"Revise os componentes e números de peça"**

Revise os componentes e números de peça dos switches de cluster 9336C-FX2 e 9336C-FX2-T.

3. **"Revise a documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 9336C-FX2 e 9336C-FX2-T e o cluster ONTAP .

4. **"Revise os requisitos do Smart Call Home"**

Revise os requisitos do recurso Cisco Smart Call Home, usado para monitorar os componentes de hardware e software na sua rede.

5. **"Instale o hardware"**

Instale o hardware do switch.

6. **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalação e manutenção dos switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de revisar os requisitos de configuração e rede.

Suporte à ONTAP

ONTAP 9.9,1 e posterior

A partir do ONTAP 9.9,1, você pode usar os switches Cisco Nexus 9336C-FX2 para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhado.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

> O monitor de integridade do switch Ethernet não suporta ONTAP 9.13.1P8 e anteriores e 9.14.1P3 e anteriores ou NX-os versão 10,3(4a)(M).

ONTAP 9.10.1 e posterior

Além disso, a partir do ONTAP 9.10.1, você pode usar os switches Cisco Nexus 9336C-FX2-T para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhada.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

Requisitos de configuração

Certifique-se de que:

- Você tem o número e o tipo apropriados de cabos e conetores de cabo para seus switches. Consulte "Hardware Universe" .
- Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo do console incluído.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para o tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700s, a interface e0M utiliza uma porta Ethernet dedicada.
- Consulte a "Hardware Universe" para obter as informações mais recentes.

Para obter mais informações sobre a configuração inicial do switch, consulte o seguinte guia: "Guia de instalação e atualização do Cisco Nexus 9336C-FX2".

O que vem a seguir

Depois de revisar os requisitos de configuração, você pode confirmar sua"componentes e números de peças" .

Componentes e números de peça para switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Para instalação e manutenção do switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de rever a lista de componentes e números de peça.

Detalhes do número de peça

A tabela a seguir lista o número de peça e a descrição dos interrutores 9336C-FX2 e 9336C-FX2BASE-T, ventiladores e fontes de alimentação:

Número de peça	Descrição
X190200-CS-PE	Interrutor de cluster, N9336C 36Pt PTSX 10/25/40/100g
X190200-CS-PI	Comutador de cluster, N9336C 36Pt PSIN 10/25/40/100g
X190212-CS-PE	Interrutor de cluster, N9336C 12pt (9336C-FX2-T) PTSX 10/25/40/100g
X190212-CS-PI	Interrutor de cluster, N9336C 12pt (9336C-FX2-T) PSIN 10/25/40/100g
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 24 portas POD licença
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Kit de acessórios X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336CA AC 1100W PSU - fluxo de ar do escape lateral da porta
X-NXA-PAC-1100W-PI2	N9K-9336CA AC 1100W PSU - fluxo de ar de entrada lateral da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, fluxo de ar do escape lateral da porta
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, fluxo de ar de admissão do lado da porta

Licenças Cisco Smart somente para portas 9336C-FX2-T

Para ativar mais de 12 portas em seu switch de cluster Cisco Nexus 9336C-FX-T, você deve comprar uma licença Cisco Smart. As licenças inteligentes da Cisco são gerenciadas por meio de contas inteligentes da Cisco.

1. Crie uma nova conta Smart, se necessário. "Crie uma nova conta inteligente"Consulte para obter detalhes.
2. Solicitar acesso a uma conta inteligente existente. "Solicitar acesso a uma conta inteligente existente"Consulte para obter detalhes.

Depois de adquirir sua licença Smart, instale o RCF apropriado para habilitar e configurar todas as 36 portas disponíveis para uso.

O que vem a seguir

Depois de confirmar seus componentes e números de peça, você revisa o"documentação necessária" .

Requisitos de documentação para switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalação e manutenção dos switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T, revise a documentação específica do switch e do controlador para configurar seus switches Cisco 9336-FX2 e o cluster ONTAP .

Documentação do switch

Para configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T, você precisa da seguinte documentação do "Suporte para switches Cisco Nexus 9000 Series" página:

Título do documento	Descrição
Guia de Instalação de hardware da Série Nexus 9000	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
Guias de configuração do software de comutador da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
Guia de atualização e downgrade do software NX-os da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
Cisco Nexus 9000 Series NX-os Guia de Referência de comando	Fornece links para as várias referências de comando fornecidas pelo Cisco.
Cisco Nexus 9000 MIBs Referência	Descreve os arquivos MIB (Management Information base) para os switches Nexus 9000.
Nexus 9000 Series NX-os System Message Reference	Descreve as mensagens do sistema para os switches da série Cisco Nexus 9000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de lançamento do Cisco Nexus 9000 Series NX-os (escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 9000 Series.
Conformidade regulamentar e informações de segurança para a série Cisco Nexus 9000	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 9000.

Documentação de sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para sua versão do sistema operacional "ONTAP 9" .

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.
Documentação do ONTAP	Fornece informações detalhadas sobre todos os aspetos das versões do ONTAP.
"Hardware Universe"	Fornece informações de compatibilidade e configuração de hardware NetApp.

Kit de trilho e documentação do gabinete

Para instalar um switch Cisco 9336-FX2 em um gabinete NetApp, consulte a documentação de hardware a seguir.

Nome	Descrição
"Armário do sistema 42U, guia profundo"	Descreve as FRUs associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição da FRU.
"Instale um switch Cisco 9336-FX2 em um gabinete NetApp"	Descreve como instalar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T em um gabinete NetApp de quatro postes.

Requisitos para Smart Call Home

Para usar o Smart Call Home, você deve configurar um switch de rede de cluster para se comunicar por e-mail com o sistema Smart Call Home. Além disso, você pode opcionalmente configurar seu switch de rede de cluster para aproveitar o recurso de suporte Smart Call Home incorporado da Cisco.

O Smart Call Home monitora os componentes de hardware e software na sua rede. Quando ocorre uma configuração crítica do sistema, ele gera uma notificação por e-mail e envia um alerta para todos os destinatários configurados no seu perfil de destino.

Antes de usar o Smart Call Home, esteja ciente dos seguintes requisitos:

- Um servidor de e-mail deve estar no lugar.
- O switch deve ter conetividade IP com o servidor de e-mail.
- É necessário configurar o nome do contacto (contacto do servidor SNMP), o número de telefone e as informações do endereço da rua. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID de CCO deve ser associado a um contrato de serviço Cisco SMARTnet apropriado para a sua empresa.

- O Serviço SMARTnet da Cisco deve estar em vigor para que o dispositivo seja registrado.

O "Site de suporte da Cisco" contém informações sobre os comandos para configurar Smart Call Home.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalar e configurar o hardware dos switches de cluster 9336C-FX2 e 9336C-FX2-T, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2. **"Instale o interrutor"**

Instale os switches 9336C-FX2 e 9336C-FX2-T.

3. **"Instale o interrutor em um gabinete NetApp"**

Instale os switches 9336C-FX2 e 9336C-FX2-T e o painel de passagem em um gabinete NetApp , conforme necessário.

4. **"Revise o cabeamento e a configuração"**

Revise o suporte para portas Ethernet NVIDIA , requisitos de FEC de 25 GbE e informações sobre recursos TCAM.

Complete a Planilha de cabeamento do Cisco Nexus 9336C-FX2 ou 9336C-FX2-T.

Se você quiser documentar as plataformas suportadas, baixe um PDF desta página e complete a Planilha de cabeamento.

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

- Planilha de cabeamento de amostra 9336C-FX2
- Folha de cálculo de cabeamento em branco 9336C-FX2
- Folha de cálculo de cabeamento de amostra 9336C-FX2BASE-T (12 portas)
- Folha de cálculo de cabeamento em branco 9336C-FX2BASE-T (12 portas)

Planilha de cabeamento de amostra 9336C-FX2

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta
1	4x10GbE nó 1	1	4x10GbE nó 1
2	4x10GbE nó 2	2	4x10GbE nó 2
3	4x10GbE nó 3	3	4x10GbE nó 3
4	4x25GbE nó 4	4	4x25GbE nó 4
5	4x25GbE nó 5	5	4x25GbE nó 5
6	4x25GbE nó 6	6	4x25GbE nó 6
7	Nó 40/100GbE 7	7	Nó 40/100GbE 7
8	Nó 40/100GbE 8	8	Nó 40/100GbE 8
9	Nó 40/100GbE 9	9	Nó 40/100GbE 9
10	Nó 40/100GbE 10	10	Nó 40/100GbE 10
11	Nó 40/100GbE 11	11	Nó 40/100GbE 11
12	Nó 40/100GbE 12	12	Nó 40/100GbE 12
13	Nó 40/100GbE 13	13	Nó 40/100GbE 13
14	Nó 40/100GbE 14	14	Nó 40/100GbE 14
15	Nó 40/100GbE 15	15	Nó 40/100GbE 15
16	Nó 40/100GbE 16	16	Nó 40/100GbE 16
17	Nó 40/100GbE 17	17	Nó 40/100GbE 17
18	Nó 40/100GbE 18	18	Nó 40/100GbE 18
19	Nó 40/100GbE 19	19	Nó 40/100GbE 19
20	Nó 40/100GbE 20	20	Nó 40/100GbE 20
21	Nó 40/100GbE 21	21	Nó 40/100GbE 21

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
22	Nó 40/100GbE 22	22	Nó 40/100GbE 22
23	Nó 40/100GbE 23	23	Nó 40/100GbE 23
24	Nó 40/100GbE 24	24	Nó 40/100GbE 24
25 a 34	Todos os direitos reservados	25 a 34	Todos os direitos reservados
35	100GbE ISL para a porta 35 do interrutor B.	35	100GbE ISL para mudar A porta 35
36	100GbE ISL para a porta 36 do interrutor B.	36	100GbE ISL para mudar A porta 36

Folha de cálculo de cabeamento em branco 9336C-FX2

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A seção *conexões de cluster suportadas* da "Hardware Universe" define as portas de cluster usadas pela plataforma.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 a 34	Todos os direitos reservados	25 a 34	Todos os direitos reservados
35	100GbE ISL para a porta 35 do interrutor B.	35	100GbE ISL para mudar A porta 35
36	100GbE ISL para a porta 36 do interrutor B.	36	100GbE ISL para mudar A porta 36

Folha de cálculo de cabeamento de amostra 9336C-FX2BASE-T (12 portas)

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta
1	4x10GbE nó 1	1	4x10GbE nó 1

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
2	4x10GbE nó 2	2	4x10GbE nó 2
3	4x10GbE nó 3	3	4x10GbE nó 3
4	4x25GbE nó 4	4	4x25GbE nó 4
5	4x25GbE nó 5	5	4x25GbE nó 5
6	4x25GbE nó 6	6	4x25GbE nó 6
7	Nó 40/100GbE 7	7	Nó 40/100GbE 7
8	Nó 40/100GbE 8	8	Nó 40/100GbE 8
9	Nó 40/100GbE 9	9	Nó 40/100GbE 9
10	Nó 40/100GbE 10	10	Nó 40/100GbE 10
11 a 34	Requer licença	11 a 34	Requer licença
35	100GbE ISL para a porta 35 do interrutor B.	35	100GbE ISL para mudar A porta 35
36	100GbE ISL para a porta 36 do interrutor B.	36	100GbE ISL para mudar A porta 36

Folha de cálculo de cabeamento em branco 9336C-FX2BASE-T (12 portas)

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A seção *conexões de cluster suportadas* da "Hardware Universe" define as portas de cluster usadas pela plataforma.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
1		1	
2		2	
3		3	
4		4	
5		5	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
6		6	
7		7	
8		8	
9		9	
10		10	
11 a 34	Requer licença	11 a 34	Requer licença
35	100GbE ISL para a porta 35 do interrutor B.	35	100GbE ISL para mudar A porta 35
36	100GbE ISL para a porta 36 do interrutor B.	36	100GbE ISL para mudar A porta 36

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você"instalar o interruptor" .

Instalar switches de cluster 9336C-FX2 e 9336C-FX2-T

Siga este procedimento para instalar e configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões NX-os e Reference Configuration File (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- "fichas de trabalho de cablagem"Concluído .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- "Documentação necessária do switch e do ONTAP".

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o…	Então…
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte o guia *Instalando um switch de cluster Cisco Nexus 9336C-FX2 e o painel pass-through em um gabinete NetApp* para obter instruções para instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.

O que se segue?

Opcionalmente, você pode"Instale um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp" . Caso contrário, vá para"revisar cabeamento e configuração" .

Instalar switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T em um gabinete NetApp

Dependendo da sua configuração, pode ser necessário instalar o switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T e o painel de passagem em um gabinete NetApp . Suportes padrão estão incluídos com o interruptor.

Antes de começar

Certifique-se de que tem o seguinte:

- O kit de painel de passagem, que está disponível na NetApp (código de peça X8784-R6).

  O kit do painel de passagem do NetApp contém o seguinte hardware:

  - Um painel obturador de passagem
  - Quatro parafusos 10-32 x .75
  - Quatro porcas de freio 10-32
- Para cada interrutor, oito parafusos 10-32 ou 12-24 e porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiros e traseiros do armário.
- O kit de trilho padrão Cisco para instalar o switch em um gabinete NetApp.

> Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

- Para obter os requisitos iniciais de preparação, o conteúdo do kit e as precauções de segurança, "Guia de instalação de hardware do Cisco Nexus 9000 Series" consulte .

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

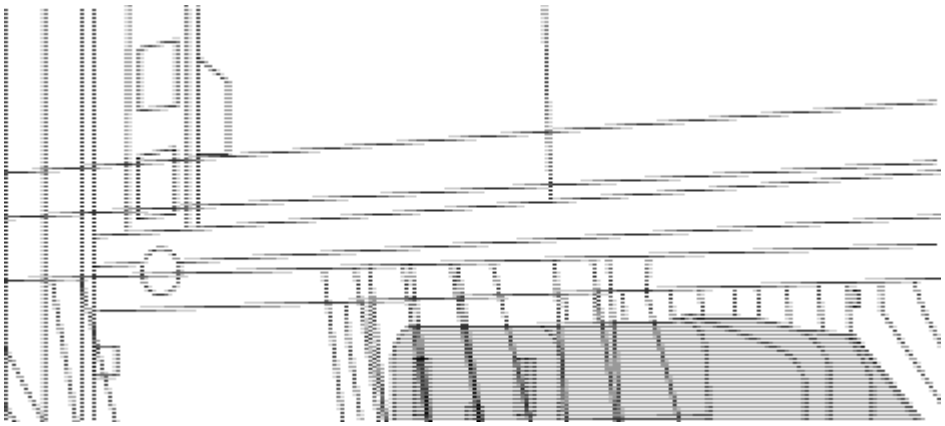
   a. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

Neste procedimento, o painel obturador é instalado no U40.

b. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

c. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

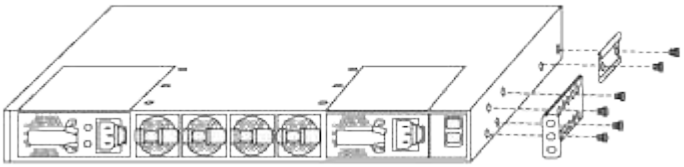
d. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.



(1) conetor fêmea do cabo de ligação em ponte.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.

a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.

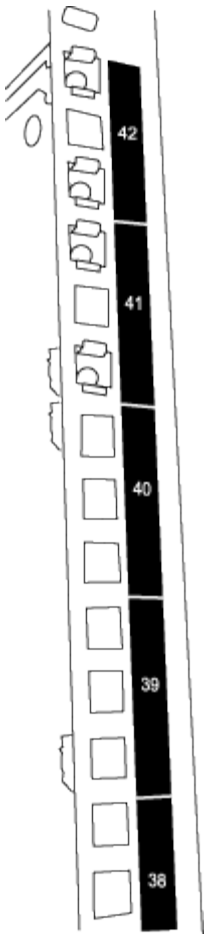


b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.

c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.

d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.

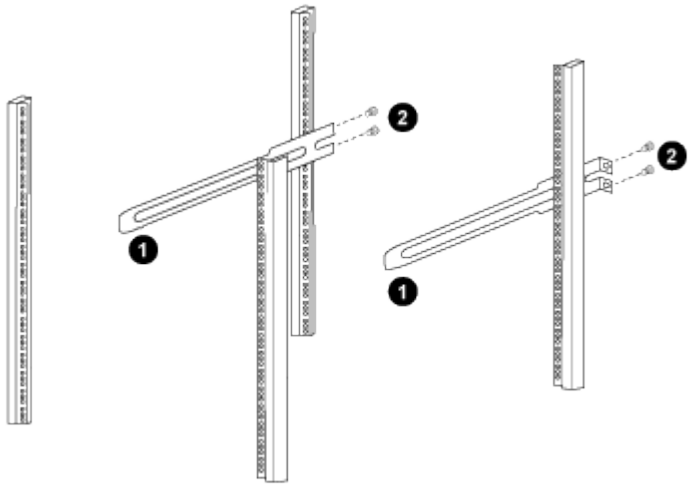
3. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



Os dois switches 9336C-FX2 e 9336C-FX2-T são sempre montados no 2U superior do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no gabinete.

   a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



(1) enquanto desliza suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.

(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

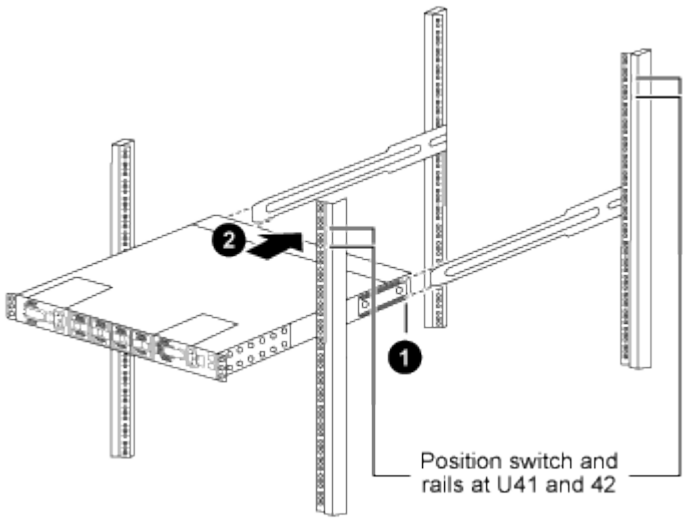
a. Repita o passo 4a para o poste traseiro do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

5. Instale o interrutor no gabinete.

> Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

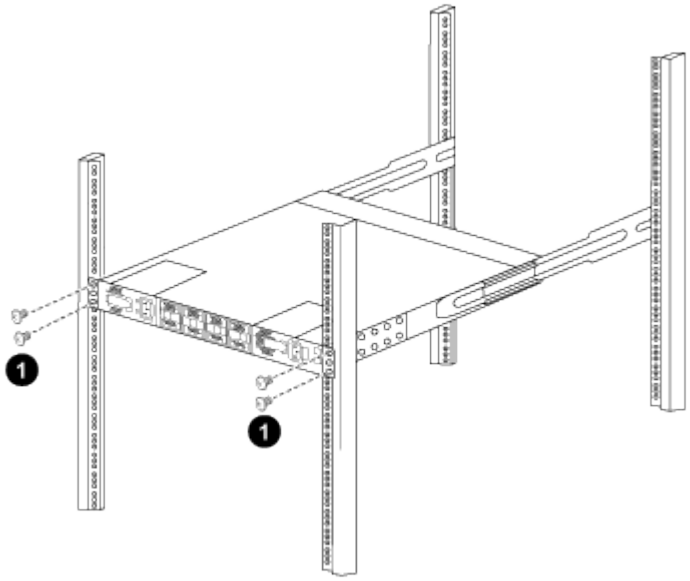
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário manter a frente do segundo interrutor durante o processo de instalação.

6. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
7. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

8. Conecte a porta de gerenciamento em cada switch 9336C-FX2 e 9336C-FX2-T a qualquer um dos switches de gerenciamento (se solicitado) ou conecte-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

O que se segue?

Depois de instalar os switches no gabinete NetApp , você"configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T" .

Analise as considerações sobre cabeamento e configuração

Antes de configurar seus switches 9336C-FX2 e 9336C-FX2-T, revise as seguintes considerações.

Suporte para portas NVIDIA CX6, CX6-DX e CX7 Ethernet

Se estiver conetando uma porta de switch a um controlador ONTAP usando as portas de NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), é necessário codificar a velocidade da porta do switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

25GbE requisitos da FEC

Portas FAS2820 e0a/e0b

As portas FAS2820 e0a e e0b exigem alterações na configuração FEC para serem vinculadas às portas de switch 9336C-FX2 e 9336C-FX2-T. Para as portas de switch e0a e e0b, a configuração fec é definida como `rs-cons16`.

```
(cs1)(config)# interface Ethernet1/8-9
(cs1)(config-if-range)# fec rs-cons16
(cs1)(config-if-range)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

As portas não se ligam devido a recursos TCAM

Nos switches 9336C-FX2 e 9336C-FX2-T, os recursos de memória endereçável de conteúdo ternário (TCAM) configurados na configuração utilizada pelo switch estão esgotados.

Consulte o artigo da base de dados de Conhecimento "As portas não se conetam no Cisco Nexus 9336C-FX2 devido aos recursos TCAM" para obter detalhes sobre como resolver este problema.

Configurar o software

Fluxo de trabalho de instalação de software para switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalar e configurar o software para os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T e para instalar ou atualizar o arquivo de configuração de referência (RCF), siga estas etapas:

1. **"Configure o interrutor"**
   Configure os switches de cluster 9336C-FX2 e 9336C-FX2-T.

2. **"Prepare-se para instalar o software NX-os e o RCF"**
   O software Cisco NX-OS e os arquivos de configuração de referência (RCFs) devem ser instalados nos switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T.

3. **"Instale ou atualize o software NX-os"**
   Baixe e instale ou atualize o software NX-OS nos switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T.

4. **"Instale ou atualize o RCF"**

Instale ou atualize o RCF após configurar os switches Cisco 9336C-FX2 e 9336C-FX2-T pela primeira vez. Você também pode usar este procedimento para atualizar sua versão do RCF.

5 **"Verifique a configuração do SSH"**

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

6 **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações dos switches de cluster 9336C-FX2 e 9336C-FX2-T.

Configurar os switches de cluster 9336C-FX2 e 9336C-FX2-T

Siga este procedimento para configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões NX-os e Reference Configuration File (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- "fichas de trabalho de cablagem"Concluído .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- "Documentação necessária do switch e do ONTAP".

Passos

1. Execute uma configuração inicial dos switches de rede do cluster.

   Forneça respostas aplicáveis às seguintes perguntas de configuração inicial ao inicializar o switch pela primeira vez. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Aviso	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com **sim**. A predefinição é não
Pretende aplicar o padrão de palavra-passe seguro? (sim/não)	Responda com **sim**. O padrão é sim.
Introduza a palavra-passe para admin.	A senha padrão é "'admin'"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.

Aviso	Resposta
Pretende introduzir a caixa de diálogo de configuração básica? (sim/não)	Responda com **sim** na configuração inicial do comutador.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em administradores alternativos. O padrão é **não**.
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com **não**. A predefinição é não
Configurar string de comunidade SNMP de leitura-escrita? (sim/não)	Responda com **não**. A predefinição é não
Introduza o nome do interrutor.	Introduza o nome do interrutor, que está limitado a 63 carateres alfanuméricos.
Continuar com a configuração de gerenciamento fora da banda (mgmt0)? (sim/não)	Responda com **yes** (o padrão) nesse prompt. No prompt mgmt0 IPv4 address:, insira seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com **sim**. No endereço IPv4 do prompt default-gateway:, digite seu default_gateway.
Configurar opções IP avançadas? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço telnet? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço SSH? (sim/não)	Responda com **sim**. O padrão é sim. O SSH é recomendado ao usar o Ethernet Switch Health Monitor (CSHM) para seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Introduza o tipo de chave SSH que pretende gerar (dsa/rsa/rsa1).	O padrão é **rsa**.
Introduza o número de bits de chave (1024-2048).	Introduza o número de bits de chave de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com **não**. A predefinição é não

Aviso	Resposta
Configurar camada de interface padrão (L3/L2)	Responda com **L2**. A predefinição é L2.
Configurar o estado predefinido da interface da porta do switch (shut/noshut)	Responda com **noshut**. O padrão é noshut.
Configurar o perfil do sistema CoPP (strict/moderate/lenient/dense)	Responda com **strict**. O padrão é rigoroso.
Pretende editar a configuração? (sim/não)	Você deve ver a nova configuração neste momento. Reveja e faça as alterações necessárias à configuração que acabou de introduzir. Responda com **no** no prompt se você estiver satisfeito com a configuração. Responda com **yes** se quiser editar as configurações.
Utilizar esta configuração e guardá-la? (sim/não)	Responda com **yes** para salvar a configuração. Isto atualiza automaticamente as imagens do Kickstart e do sistema. Se você não salvar a configuração nesta fase, nenhuma das alterações entrará em vigor na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração que você fez no visor que aparece no final da configuração e certifique-se de salvar a configuração.
3. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software suportada pelo NetApp para os switches a partir da "Transferência do software Cisco" página.

O que se segue?

Depois de configurar seus switches, você"prepare-se para instalar o software NX-OS e RCF" .

Prepare-se para instalar o software NX-os e o RCF

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Documentação sugerida

- "Página do switch Ethernet Cisco"

  Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

- "Guias de atualização e downgrade de software"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

- "Atualização do Cisco Nexus 9000 e 3000 e Matriz ISSU"

Fornece informações sobre atualização/downgrade disruptiva para o software Cisco NX-os em switches Nexus 9000 Series com base em suas versões atuais e de destino.

Na página, selecione **Atualização disruptiva** e selecione sua versão atual e liberação de destino na lista suspensa.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01 e cluster1-02.
- Os nomes de LIF de cluster são 02-01_clus1 e cluster1-01_clus2 para cluster1-01 e cluster1-02_clus1 e cluster1-02_clus2 para cluster1-cluster1.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   network device-discovery show -protocol cdp
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C

4 entries were displayed.
```

4. Verifique o status administrativo ou operacional de cada interface de cluster.
   a. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Exibir informações sobre os LIFs:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o comando de reversão automática está ativado em todas as LIFs do cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

O que se segue?

Depois de se preparar para instalar o software NX-OS e o RCF, você"instalar ou atualizar o software NX-OS" .

Instale ou atualize o software NX-os

Siga este procedimento para instalar ou atualizar o software NX-OS nos switches de cluster Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar, conclua o procedimento em "Prepare-se para instalar o NX-os e o RCF".

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- "Página do switch Ethernet Cisco"

  Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

- "Guias de atualização e downgrade de software"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

- "Atualização do Cisco Nexus 9000 e 3000 e Matriz ISSU"

  Fornece informações sobre atualização/downgrade disruptiva para o software Cisco NX-os em switches Nexus 9000 Series com base em suas versões atuais e de destino.

Na página, selecione **Atualização disruptiva** e selecione sua versão atual e liberação de destino na lista suspensa.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-03_clus1 , cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.
- O `cluster1::*>` prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch pode alcançar o servidor no endereço IP 172.19.2.1:

   ```
   cs2# ping 172.19.2.1 VRF management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Copie o software NX-os e as imagens EPLD para o switch Nexus 9336C-FX2.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.5.bin  /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time:  05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 02:28:31]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS



Compatibility check is done:
Module  Bootable  Impact          Install-type  Reason
------  --------  --------------- ------------  ---------
  1     yes       Disruptive      Reset         Default upgrade is
not hitless



Images will be upgraded according to following table:

Module   Image    Running-Version(pri:alt)                New-
Version         Upg-Required
-------  -------- ----------------------------------------
-------------------- ------------
  1      nxos     9.3(4)                                  9.3(5)
yes
  1      bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)      yes
```

```
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.
```

9. Verifique a nova versão do software NX-os depois que o switch reiniciar:

   `show version`

Mostrar exemplo

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.3(5)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

10. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x17
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2

cs2# 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.
```

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

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x19
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
```

12. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -role cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
```

```
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

13. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

14. Repita os passos 6 a 13 para instalar o software NX-os no interrutor CS1.
15. Ative a reversão automática nos LIFs do cluster.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

16. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que se segue?

Depois de instalar ou atualizar o software NX-OS, você"instalar ou atualizar o arquivo de configuração de referência (RCF)" .

Instale ou atualize o RCF

Instale ou atualize a visão geral do ficheiro de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches

Nexus 9336C-FX2 e 9336C-FX2-T pela primeira vez. Você atualiza sua versão RCF quando tem uma versão existente do arquivo RCF instalada no seu switch.

Consulte o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota"para obter mais informações ao instalar ou atualizar o RCF.

Configurações RCF disponíveis

A tabela a seguir descreve os RCFs disponíveis para diferentes configurações. Escolha o RCF aplicável à sua configuração.

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

Nome RCF	Descrição
2-Cluster-HA-Breakout	É compatível com dois clusters de ONTAP com pelo menos oito nós, incluindo nós que usam portas de cluster compartilhado.
4-Cluster-HA-Breakout	Dá suporte a quatro clusters ONTAP com pelo menos quatro nós, incluindo nós que usam portas de cluster compartilhado de alta disponibilidade.
1-cluster-HA	Todas as portas são configuradas para 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas. Necessário para sistemas AFF A320, AFF A250 e FAS500f. Além disso, todas as portas podem ser usadas como portas de cluster dedicadas.
1-Cluster-HA-Breakout	As portas são configuradas para conexões de 4x10GbE, conexões de 4x25GbE (RCF 1,6 em switches 100GbE) e 40/100GbE. Dá suporte ao tráfego compartilhado de cluster/HA em portas para nós que usam portas compartilhadas de cluster/HA: Sistemas AFF A320, AFF A250 e FAS500f. Além disso, todas as portas podem ser usadas como portas de cluster dedicadas.
Cluster-HA-Storage	As portas são configuradas para 40/100GbE para cluster e HA, 4 x 10 GbE breakout para cluster e 4 x 25 GbE breakout para cluster e HA, e 100GbE para cada par de HA de storage.
Cluster	Dois tipos de RCF com diferentes alocações de portas 4x10GbE (breakout) e portas 40/100GbE. Todos os nós FAS/AFF são compatíveis, exceto nos sistemas AFF A320, AFF A250 e FAS500f.
Armazenamento	Todas as portas são configuradas para 100GbE conexões de storage NVMe.

Documentação sugerida

- "Switches Ethernet Cisco (NSS)"

  Consulte a tabela de compatibilidade de switch para ver as versões ONTAP e RCF suportadas no site de suporte da NetApp. Note que pode haver dependências de comando entre a sintaxe de comando no RCF

e a sintaxe encontrada em versões específicas do NX-os.

- "Switches Cisco Nexus 3000 Series"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são **CS1** e **CS2**.
- Os nomes dos nós são **cluster1-01**, **cluster1-02**, **cluster1-03** e **cluster1-04**.
- Os nomes de cluster LIF são **cluster1-01_clus1**, **cluster1-01_clus2**, **cluster1-03_clus2**, **cluster1-03_clus1**, **cluster1-02_clus2**, **cluster1-02_clus1**, **cluster1-04_clus1** e **cluster1-04_clus2**.
- O `cluster1::*>` prompt indica o nome do cluster.

Os exemplos neste procedimento usam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE **e0a** e **e0b**. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Para obter detalhes sobre as configurações de RCF disponíveis, "Fluxo de trabalho de instalação do software"consulte .

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

O que se segue?

Depois de revisar o procedimento de instalação do RCF ou atualização do RCF, você"instalar o RCF" ou"atualize seu RCF" conforme necessário.

Instalar o ficheiro de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches Nexus 9336C-FX2 e 9336C-FX2-T pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma ligação de consola ao interrutor. A conexão do console é opcional se você tiver acesso remoto ao switch.
- O switch CS1 e o switch CS2 são ativados e a configuração inicial do switch está concluída (o endereço IP de gerenciamento e o SSH são configurados).
- A versão NX-os pretendida foi instalada.
- As ligações ISL entre os interrutores estão ligadas.
- As portas do cluster de nós do ONTAP não estão conetadas.

Passo 1: Instale o RCF nos interrutores

1. Faça login no switch CS1 usando SSH ou usando um console serial.
2. Copie o RCF para o flash de inicialização do switch CS1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 9000 Series NX-os" guias.

   Mostrar exemplo

   Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS1:

   ```
   cs1# copy tftp: bootflash: vrf management
   Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
   Enter hostname for the tftp server: 172.22.201.50
   Trying to connect to tftp server......Connection to Server
   Established.
   TFTP get operation was successful
   Copy complete, now saving to disk (please wait)...
   ```

3. Aplique o RCF baixado anteriormente ao flash de inicialização.

   Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 9000 Series NX-os" guias.

   Mostrar exemplo

   Este exemplo mostra o arquivo RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` sendo instalado no switch CS1:

   ```
   cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
   config echo-commands
   ```

4. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs1# show banner motd

*****************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Nexus N9K-C9336C-FX2
* Filename : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : 10-23-2020
* Version  : v1.6
*
* Port Usage:
* Ports  1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports  4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports  7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****************************************************************
**********
```

5. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

  A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.
7. Depois de verificar se as versões RCF e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

```
cs1# copy running-config startup-config
[########################################] 100% Copy complete
```

8. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

   Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

10. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

11. Emitir o `write erase` comando para apagar a configuração salva atual:

```
cs1# write erase
```

```
Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

12. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config.
```

13. Interrutor de reinicialização CS1.

```
cs1# reload

This command will reboot the system. (y/n)? [n] y
```

14. Repita os passos 1 a 13 no switch cs2.
15. Conecte as portas do cluster de todos os nós do cluster ONTAP aos switches CS1 e CS2.

Etapa 2: Verifique as conexões do interrutor

1. Verifique se as portas do switch conetadas às portas do cluster estão **up**.

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

2. Verifique se os nós de cluster estão em suas VLANs de cluster corretas usando os seguintes comandos:

```
show vlan brief

show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

```
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         active    Eth1/11, Eth1/12,
Eth1/13
                                                  Eth1/14, Eth1/15,
Eth1/16
                                                  Eth1/17, Eth1/18,
Eth1/19
                                                  Eth1/20, Eth1/21,
Eth1/22
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34

cs1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
----------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
Eth1/9/1      1       trunking      --
Eth1/9/2      1       trunking      --
Eth1/9/3      1       trunking      --
Eth1/9/4      1       trunking      --
Eth1/10/1     1       trunking      --
Eth1/10/2     1       trunking      --
Eth1/10/3     1       trunking      --
Eth1/10/4     1       trunking      --
Eth1/11       33      trunking      --
```

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

```
Eth1/11       31,33
Eth1/12       31,33
Eth1/13       31,33
Eth1/14       31,33
Eth1/15       31,33
Eth1/16       31,33
Eth1/17       31,33
Eth1/18       31,33
Eth1/19       31,33
Eth1/20       31,33
Eth1/21       31,33
Eth1/22       31,33
Eth1/23       32,34
Eth1/24       32,34
Eth1/25       32,34
Eth1/26       32,34
Eth1/27       32,34
Eth1/28       32,34
Eth1/29       32,34
Eth1/30       32,34
Eth1/31       32,34
Eth1/32       32,34
Eth1/33       32,34
Eth1/34       32,34
Eth1/35       1
Eth1/36       1
Po1           1
..
..
..
..
..
```

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

3. Verifique se o ISL entre CS1 e CS2 está funcional:

```
show port-channel summary
```

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

Passo 3: Configure o cluster do ONTAP

A NetApp recomenda que você use o Gerenciador de sistemas para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e configuração de cluster, incluindo a atribuição de um endereço IP de gerenciamento de nós, a inicialização do cluster, a criação de um nível local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Aceda a "Configure o ONTAP em um novo cluster com o Gerenciador do sistema" para obter instruções de configuração.

O que se segue?

Depois de instalar o RCF, você"verificar a configuração SSH" .

Atualizar o seu ficheiro de configuração de referência (RCF)

Você atualiza sua versão RCF quando você tem uma versão existente do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual.
- Se você estiver atualizando sua versão do RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se você precisar alterar a configuração de inicialização para refletir as imagens de inicialização atuais, você deve fazê-lo antes de reaplicar o RCF para que a versão correta seja instanciada em futuras reinicializações.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Antes de instalar uma nova versão do software do switch e RCFs, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Passo 1: Prepare-se para a atualização

1. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show –role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90    N9K-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

3. Desative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
false
```

Etapa 2: Configurar portas

1. No switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

```
cs1(config)# interface eth1/1/1-2,eth1/7-8

cs1(config-if-range)# shutdown
```

> Certifique-se de encerrar **todas** portas de cluster conetadas para evitar quaisquer problemas de conexão de rede. Consulte o artigo da base de dados de Conhecimento "Nó fora do quórum ao migrar LIF do cluster durante a atualização do SO do switch" para obter mais detalhes.

2. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

   `network interface show -role cluster`

   Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
8 entries were displayed.
cluster1::*>
```

3. Verifique se o cluster está em bom estado:

   `cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

4. Se você ainda não fez isso, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

   `show running-config`

   a. Registre quaisquer adições personalizadas entre o atual `running-config` e o arquivo RCF em uso (como uma configuração SNMP para sua organização).

   b. A partir do NX-OS 10.2, use o `show diff running-config` comando para comparar com o arquivo RCF salvo no bootflash. Caso contrário, use uma ferramenta de comparação/diferenciação de terceiros.

5. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

   ```
   cs1# show run | i "username admin password" > bootflash:write_erase.cfg

   cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

   cs1# show run | section "switchname" >> bootflash:write_erase.cfg
   ```

6. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

   ```
   cs1# echo "hardware access-list tcam region ing-racl 1024" >>
   bootflash:write_erase.cfg

   cs1# echo "hardware access-list tcam region egr-racl 1024" >>
   bootflash:write_erase.cfg

   cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
   bootflash:write_erase.cfg
   ```

   Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

7. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Emita o comando write erase para apagar a configuração salva atual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

9. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Execute uma reinicialização do switch:

```
switch# reload

This command will reboot the system. (y/n)? [n] y
```

11. Depois que o endereço IP de gerenciamento for acessível novamente, faça login no switch através de SSH.

    Talvez seja necessário atualizar as entradas do arquivo host relacionadas às chaves SSH.

12. Copie o RCF para o flash de inicialização do switch CS1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

    Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 9000 Series NX-os" guias.

    Mostrar exemplo

    Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server......Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

13. Aplique o RCF baixado anteriormente ao flash de inicialização.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 9000 Series NX-os" nos guias.

Mostrar exemplo

Este exemplo mostra o arquivo RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` sendo instalado no switch CS1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

14. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs1# show banner motd

*****************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Nexus N9K-C9336C-FX2
* Filename : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : 10-23-2020
* Version  : v1.6
*
* Port Usage:
* Ports  1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports  4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports  7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****************************************************************
**********
```

15. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

  A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

16. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
17. Depois de verificar se as versões RCF, adições personalizadas e configurações de switch estão corretas, copie o arquivo running-config para o arquivo startup-config.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 9000 Series NX-os" nos guias.

    ```
    cs1# copy running-config startup-config

    [] 100% Copy complete
    ```

18. Interrutor de reinicialização CS1. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e eventos de portas de cluster down" relatados nos nós enquanto o switch for reinicializado.

    ```
    cs1# reload

    This command will reboot the system. (y/n)? [n] y
    ```

19. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

       ```
       network port show -role cluster
       ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ---------------
-----
cs1                         cluster-network    10.233.205.90    NX9-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    NX9-
```

```
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

20. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

21. Repita os passos 1 a 20 no interrutor CS2.
22. Ative a reversão automática nos LIFs do cluster.

    `cluster1::*> **network interface modify -vserver Cluster -lif * -auto-revert True**`

Etapa 3: Verifique a configuração da rede do cluster e a integridade do cluster

1. Verifique se as portas do switch conetadas às portas do cluster estão **up**.

   ```
   show interface brief
   ```

   Mostrar exemplo

   ```
   cs1# show interface brief | grep up
   .
   .
   Eth1/1/1      1       eth  access up      none
   10G(D) --
   Eth1/1/2      1       eth  access up      none
   10G(D) --
   Eth1/7        1       eth  trunk  up      none
   100G(D) --
   Eth1/8        1       eth  trunk  up      none
   100G(D) --
   .
   .
   ```

2. Verifique se os nós esperados ainda estão conetados:

   ```
   show cdp neighbors
   ```

Mostrar exemplo

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Verifique se os nós de cluster estão em suas VLANs de cluster corretas usando os seguintes comandos:

   `show vlan brief`

   `show interface trunk`

Mostrar exemplo

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

```
                                                    Eth1/26, Eth1/27,
Eth1/28
                                                    Eth1/29, Eth1/30,
Eth1/31
                                                    Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         active    Eth1/11, Eth1/12,
Eth1/13
                                                    Eth1/14, Eth1/15,
Eth1/16
                                                    Eth1/17, Eth1/18,
Eth1/19
                                                    Eth1/20, Eth1/21,
Eth1/22
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                    Eth1/26, Eth1/27,
Eth1/28
                                                    Eth1/29, Eth1/30,
Eth1/31
                                                    Eth1/32, Eth1/33,
Eth1/34

cs1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
----------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
Eth1/9/1      1       trunking      --
Eth1/9/2      1       trunking      --
Eth1/9/3      1       trunking      --
Eth1/9/4      1       trunking      --
Eth1/10/1     1       trunking      --
Eth1/10/2     1       trunking      --
Eth1/10/3     1       trunking      --
Eth1/10/4     1       trunking      --
Eth1/11       33      trunking      --
```

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

```
Eth1/11       31,33
Eth1/12       31,33
Eth1/13       31,33
Eth1/14       31,33
Eth1/15       31,33
Eth1/16       31,33
Eth1/17       31,33
Eth1/18       31,33
Eth1/19       31,33
Eth1/20       31,33
Eth1/21       31,33
Eth1/22       31,33
Eth1/23       32,34
Eth1/24       32,34
Eth1/25       32,34
Eth1/26       32,34
Eth1/27       32,34
Eth1/28       32,34
Eth1/29       32,34
Eth1/30       32,34
Eth1/31       32,34
Eth1/32       32,34
Eth1/33       32,34
Eth1/34       32,34
Eth1/35       1
Eth1/36       1
Po1           1
..
..
..
..
..
```

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

4. Verifique se o ISL entre CS1 e CS2 está funcional:

```
show port-channel summary
```

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

5. Verifique se os LIFs do cluster reverteram para sua porta inicial:

   `network interface show -role cluster`

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver vserver_name -lif lif_name`

6. Verifique se o cluster está em bom estado:

`cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------- -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

7. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

O que se segue?

Depois de atualizar seu RCF, você"verificar a configuração SSH" .

Verifique a configuração da SSH

Se você estiver usando os recursos CSHM (Ethernet Switch Health Monitor) e coleta de

logs, verifique se as chaves SSH e SSH estão habilitadas nos switches de cluster.

Passos

1. Verifique se o SSH está ativado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verifique se as chaves SSH estão ativadas:

```
show ssh key
```

Mostrar exemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Ao ativar o FIPS, você deve alterar o número de bits para 256 na central usando o comando `ssh key ecdsa 256 force`. "Configurar a segurança da rede usando o FIPS"Consulte para obter mais detalhes.

O que se segue?

Depois de verificar sua configuração SSH, você"configurar monitoramento de integridade do switch" .

Redefinir os switches do cluster 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica

Para redefinir os switches de cluster 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica, você deve apagar as configurações dos switches 9336C-FX2 e 9336C-FX2-T.

Sobre esta tarefa

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

Passos

1. Apagar a configuração existente:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Recarregue o software do switch:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   O sistema é reinicializado e entra no assistente de configuração. Durante a inicialização, se você receber o prompt “Abortar provisionamento automático e continuar com a configuração normal? (sim/não)[n]”, você deve responder **sim** para prosseguir.

Migrar os switches

Migrar de switches de cluster NetApp CN1610 para switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T

Você pode migrar switches de cluster NetApp CN1610 para um cluster ONTAP para switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T. Este é um procedimento não disruptivo.

Rever os requisitos

Você deve estar ciente de determinadas informações de configuração, conexões de porta e requisitos de cabeamento ao substituir switches de cluster NetApp CN1610 por switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T. Você também deve verificar o número de série do switch para garantir que o switch correto seja migrado.

Interrutores suportados

Os seguintes switches de cluster são suportados:

- NetApp CN1610
- Cisco 9336C-FX2
- Cisco 9336C-FX2-T

Para obter detalhes sobre as portas suportadas e suas configurações, consulte o "Hardware Universe".

O que você vai precisar

Verifique se sua configuração atende aos seguintes requisitos:

- O cluster existente está corretamente configurado e funcionando.
- Todas as portas de cluster estão no estado **up** para garantir operações ininterruptas.
- Os switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T estão configurados e operando sob a versão correta do NX-OS instalada com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede de cluster existente tem o seguinte:
  - Um cluster NetApp redundante e totalmente funcional usando switches NetApp CN1610.
  - Conetividade de gerenciamento e acesso ao console aos switches NetApp CN1610 e aos novos switches.
  - Todas as LIFs de cluster no estado up com os LIFs de cluster estão em suas portas residenciais.
- Algumas portas são configuradas nos switches Cisco 9336C-FX2 e 9336C-FX2-T para operar em 40GbE ou 100GbE.
- Você planejou, migrou e documentou a conectividade de 40 GbE e 100 GbE dos nós para os switches de cluster Cisco 9336C-FX2 e 9336C-FX2-T.

Migrar os switches

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de cluster CN1610 existentes são *C1* e *C2*.
- Os novos switches de cluster 9336C-FX2 são *CS1* e *CS2*.
- Os nós são *node1* e *node2*.
- Os LIFs de cluster são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *E3A* e *e3b*.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O interrutor C2 é substituído primeiro pelo interrutor CS2.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
    - Todas as LIFs do cluster fazem failover para o novo switch CS2.

- O cabeamento entre os nós e o C2 é desconetado do C2 e reconetado ao CS2.

- O interrutor C1 é substituído pelo interrutor CS1.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
    - Todas as LIFs do cluster fazem failover para o novo switch CS1.
  - O cabeamento entre os nós e o C1 é desconetado do C1 e reconetado ao CS1.

> Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir faz failover de todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

3. Desative a reversão automática nos LIFs do cluster.

   Ao desativar a reversão automática para este procedimento, as LIFs do cluster não serão automaticamente movidas de volta para sua porta inicial. Eles permanecem na porta atual enquanto continua a estar operacional.

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

Etapa 2: Configurar portas e cabeamento

1. Determine o status administrativo ou operacional de cada interface de cluster.

   Cada porta deve ser exibida durante `Link` e `healthy` para `Health Status`.

   a. Exibir os atributos da porta de rede:

      ```
      network port show -ipspace Cluster
      ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

b. Exibir informações sobre os LIFs e seus nós iniciais designados:

`network interface show -vserver Cluster`

Cada LIF deve ser exibido `up/up` para `Status Admin/Oper` e `true` para `Is Home`.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. As portas de cluster em cada nó são conetadas aos switches de cluster existentes da seguinte maneira (da perspetiva dos nós) usando o comando:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e3a    C1 (6a:ad:4f:98:3b:3f)    0/1               -
            e3b    C2 (6a:ad:4f:98:4c:a4)    0/1               -
node2      /cdp
            e3a    C1 (6a:ad:4f:98:3b:3f)    0/2               -
            e3b    C2 (6a:ad:4f:98:4c:a4)    0/2               -
```

3. As portas e os switches do cluster são conetados da seguinte maneira (da perspetiva dos switches) usando o comando:

   `show cdp neighbors`

Mostrar exemplo

```
C1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3a
node2                 Eth1/2        124    H           AFF-A400
e3a
C2                    0/13          179    S I s       CN1610
0/13
C2                    0/14          175    S I s       CN1610
0/14
C2                    0/15          179    S I s       CN1610
0/15
C2                    0/16          175    S I s       CN1610
0/16

C2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
C1                    0/13          175    S I s       CN1610
0/13
C1                    0/14          175    S I s       CN1610
0/14
C1                    0/15          175    S I s       CN1610
0/15
C1                    0/16          175    S I s       CN1610
0/16
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. no switch C2, encerre as portas conetadas às portas do cluster dos nós para fazer failover dos LIFs do cluster.

   Não tente migrar manualmente as LIFs de cluster.

   ```
   (C2)# configure
   (C2)(Config)# interface 0/1-0/12
   (C2)(Interface 0/1-0/12)# shutdown
   (C2)(Interface 0/1-0/12)# exit
   (C2)(Config)# exit
   ```

2. Mova as portas do cluster de nós do antigo switch C2 para o novo switch cs2, usando o cabeamento apropriado suportado pelo Cisco 9336C-FX2 e 9336C-FX2-T.
3. Exibir os atributos da porta de rede:

   ```
   network port show -ipspace Cluster
   ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

4. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e3a    C1  (6a:ad:4f:98:3b:3f)   0/1
CN1610
            e3b    cs2 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1     N9K-
C9336C-FX2
node2      /cdp
            e3a    C1  (6a:ad:4f:98:3b:3f)   0/2
CN1610
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2     N9K-
C9336C-FX2
```

5. No switch CS2, verifique se todas as portas do cluster de nós estão ativas:

   `network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interfac     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.3.4/16     node1
e0b     false
            node1_clus2  up/up      169.254.3.5/16     node1
e0b     true
            node2_clus1  up/up      169.254.3.8/16     node2
e0b     false
            node2_clus2  up/up      169.254.3.9/16     node2
e0b     true
```

6. No switch C1, encerre as portas conetadas às portas do cluster dos nós para fazer failover das LIFs do cluster.

```
(C1)# configure
(C1)(Config)# interface 0/1-0/12
(C1)(Interface 0/1-0/12)# shutdown
(C1)(Interface 0/1-0/12)# exit
(C1)(Config)# exit
```

7. Mova as portas do cluster de nós do antigo switch C1 para o novo switch cs1, usando o cabeamento apropriado suportado pelo Cisco 9336C-FX2 e 9336C-FX2-T.
8. Verifique a configuração final do cluster:

   `network port show -ipspace Cluster`

   Cada porta deve ser exibida `up` para `Link` e `healthy` para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

9. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /cdp
            e3a    cs1 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1   N9K-
C9336C-FX2
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
node2      /cdp
            e3a    cs1 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1   N9K-
C9336C-FX2
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
```

10. Nos switches CS1 e CS2, verifique se todas as portas do cluster de nós estão ativas:

    `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

11. Verifique se ambos os nós têm uma conexão com cada switch:

    `network device-discovery show -protocol`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
--------------
node1      /cdp
            e0a    cs1 (b8:ce:f6:19:1b:42)   Ethernet1/1/1   N9K-
C9336C-FX2
            e0b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2

node2      /cdp
            e0a    cs1 (b8:ce:f6:19:1b:42)   Ethernet1/1/1   N9K-
C9336C-FX2
            e0b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
```

Etapa 3: Verifique a configuração

1. Ativar a reversão automática nos LIFs do cluster:

   ```
   cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
   true
   ```

2. Verifique se todas as LIFs de rede do cluster estão de volta em suas portas domésticas:

   ```
   network interface show
   ```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
```

3. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

4. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

O que se segue?

Depois de migrar seus switches, você"configurar monitoramento de integridade do switch" .

Migrar de switches Cisco mais antigos para switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Você pode executar uma migração sem interrupções de switches de cluster Cisco mais antigos para switches de rede de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Rever os requisitos

Certifique-se de que:

- Você verificou o número de série do switch para garantir que o switch correto seja migrado.
- Algumas das portas nos switches Nexus 9336C-FX2 estão configuradas para serem executadas em 10GbE ou 40GbE.
- A conectividade 10GbE GbE e 40GbE de nós para switches de cluster Nexus 9336C-FX2 foi planejada, migrada e documentada.
- O cluster está totalmente funcionando (não deve haver erros nos logs ou problemas semelhantes).

- A personalização inicial dos switches Cisco Nexus 9336C-FX2 está concluída, de modo que:
  - Os switches 9336C-FX2 estão executando a versão mais recente recomendada do software.
  - Confirme se os arquivos de configuração de referência (RCFs) foram totalmente aplicados a quaisquer novos switches antes de migrar os LIFs para os novos switches.
  - Verifique as configurações de execução e inicialização em ambos os switches antes de mudar o tráfego de rede.
  - Qualquer personalização de site, como DNS, NTP, SMTP, SNMP e SSH, é configurada nos novos switches.
- Você tem acesso à tabela de compatibilidade de switch na "Switches Ethernet Cisco" página para as versões ONTAP, NX-os e RCF suportadas.
- Você analisou o software apropriado e os guias de atualização disponíveis no site da Cisco para obter os procedimentos de atualização e downgrade do switch Cisco na "Suporte para switches Cisco Nexus 9000 Series" página.

> Se você estiver alterando a velocidade da porta das portas de cluster e0a e e1a em sistemas AFF A800 ou AFF C800, você pode observar pacotes mal formados sendo recebidos após a conversão de velocidade. Consulte "Erro 1570339" e o artigo da base de dados de Conhecimento "Erros de CRC em portas T6 após a conversão de 40GbE para 100GbE" para obter orientação.

Migrar os switches

Sobre os exemplos

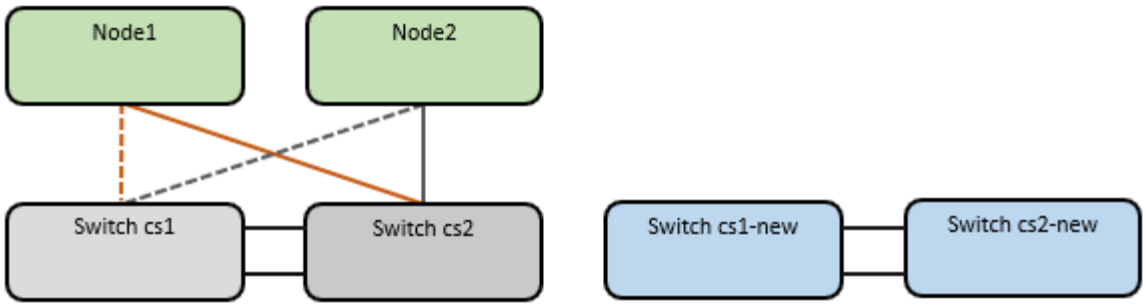
Os exemplos neste procedimento usam dois nós. Esses nós usam duas portas de interconexão de cluster 10GbE e0a e e0b. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

> As saídas de comando podem variar dependendo das diferentes versões do ONTAP.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco existentes são **CS1** e **CS2**
- Os novos switches de cluster Nexus 9336C-FX2 são **CS1-novo** e **CS2-novo**.
- Os nomes dos nós são **node1** e **node2**.
- Os nomes de LIF do cluster são **node1_clus1** e **node1_clus2** para o nó 1 e **node2_clus1** e **node2_clus2** para o nó 2.
- O prompt **cluster1::>*** indica o nome do cluster.

Durante este procedimento, consulte o seguinte exemplo:



Sobre esta tarefa

O procedimento requer o uso de comandos e comandos ONTAP "Switches Nexus 9000 Series"; comandos ONTAP são usados, salvo indicação em contrário.

Este procedimento abrange o seguinte cenário:

- O interrutor CS2 é substituído pelo interrutor CS2-novo primeiro.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
    - Todas as LIFs de cluster fazem failover para o novo switch CS2-novo.
  - O cabeamento entre os nós e o CS2 é desconetado do CS2 e reconetado ao CS2 novo.
- O interrutor CS1 é substituído pelo interrutor CS1-novo.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
    - Todas as LIFs de cluster fazem failover para o novo switch CS1-novo.
  - O cabeamento entre os nós e o CS1 é desconetado do CS1 e reconetado ao CS1 novo.

> Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir faz failover de todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde *x* é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

É apresentado o aviso avançado (*>).

Etapa 2: Configurar portas e cabeamento

1. Nos novos switches, confirme se o ISL está cabeado e funcionando entre os switches CS1-novo e CS2-novo:

   ```
   show port-channel summary
   ```

   Mostrar exemplo

   ```
   cs1-new# show port-channel summary
   Flags:  D - Down        P - Up in port-channel (members)
           I - Individual  H - Hot-standby (LACP only)
           s - Suspended   r - Module-removed
           b - BFD Session Wait
           S - Switched    R - Routed
           U - Up (port-channel)
           p - Up in delay-lacp mode (member)
           M - Not in use. Min-links not met
   ------------------------------------------------------------------------
   ------------
   Group Port-       Type     Protocol  Member Ports
         Channel
   ------------------------------------------------------------------------
   ------------
   1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

   cs2-new# show port-channel summary
   Flags:  D - Down        P - Up in port-channel (members)
           I - Individual  H - Hot-standby (LACP only)
           s - Suspended   r - Module-removed
           b - BFD Session Wait
           S - Switched    R - Routed
           U - Up (port-channel)
           p - Up in delay-lacp mode (member)
           M - Not in use. Min-links not met
   ------------------------------------------------------------------------
   ------------
   Group Port-       Type     Protocol  Member Ports
         Channel
   ------------------------------------------------------------------------
   ------------
   1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
   ```

2. Exiba as portas do cluster em cada nó conetado aos switches do cluster existentes:

   `network device-discovery show`

   Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
node2      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
```

3. Determine o status administrativo ou operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

b. Verifique se todas as interfaces de cluster (LIFs) estão em suas portas iniciais:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------
----------- ------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.233.205.92    N5K-
C5596UP
      Serial Number: FOXXXXXXXGS
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP

cs2                         cluster-network     10.233.205.93   N5K-
C5596UP
      Serial Number: FOXXXXXXXGD
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP
```

4. Desativar reversão automática nos LIFs do cluster.

   Ao desativar a reversão automática para este procedimento, as LIFs do cluster não serão automaticamente movidas de volta para sua porta inicial. Eles permanecem na porta atual enquanto continua a estar operacional.

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

   A desativação da reversão automática garante que o ONTAP somente falhe sobre as LIFs do cluster quando as portas do switch são desativadas mais tarde.

5. No switch de cluster CS2, encerre as portas conetadas às portas de cluster de **todos** os nós para fazer failover dos LIFs de cluster:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

6. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster`

   Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------ ----------
------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/16     node1
e0a     true
            node1_clus2   up/up      169.254.3.5/16     node1
e0a     false
            node2_clus1   up/up      169.254.3.8/16     node2
e0a     true
            node2_clus2   up/up      169.254.3.9/16     node2
e0a     false
```

7. Verifique se o cluster está em bom estado:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

8. Se as LIFs de cluster tiverem falhado ao switch CS1 e o cluster estiver em bom estado, vá para Passo. 10. Se algumas LIFs de cluster não estiverem íntegras ou se o cluster não estiver saudável, você poderá reverter a conetividade para o switch CS2, da seguinte forma:

   a. Abra as portas conetadas às portas de cluster de **todos** os nós:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# no shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

   b. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
---------- ------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/16     node1
e0a     true
            node1_clus2   up/up      169.254.3.5/16     node1
e0a     false
            node2_clus1   up/up      169.254.3.8/16     node2
e0a     true
            node2_clus2   up/up      169.254.3.9/16     node2
e0a     false
```

   c. Verifique se o cluster está em bom estado:

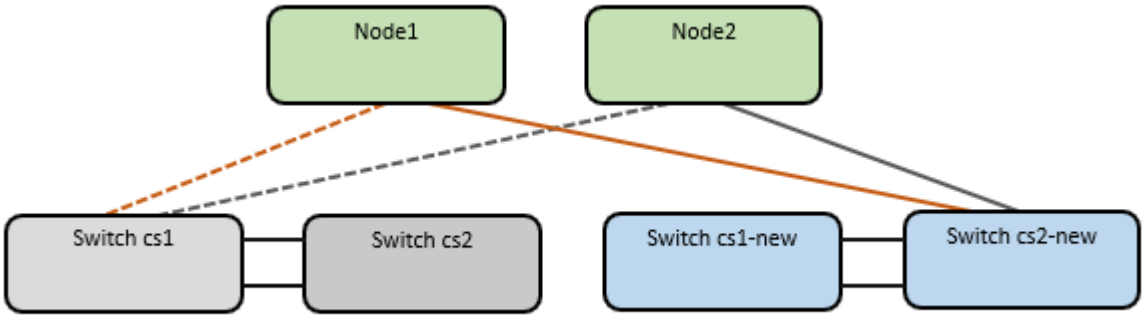
```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

9. Depois de restaurar o LIF e a integridade do cluster, reinicie o processo a partir Passo. 4do .
10. mova todos os cabos de conexão de nó do cluster do antigo switch CS2 para o novo switch de CS2 novos.

Os cabos de conexão do nó de cluster foram movidos para o switch de CS2 novo



11. Confirme a integridade das conexões de rede movidas para CS2-new:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Todas as portas de cluster que foram movidas devem estar para cima.

12. Verifique as informações do vizinho nas portas do cluster:

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
--------------
node1      /cdp
            e0a    cs1                       Ethernet1/1    N5K-
C5596UP
            e0b    cs2-new                   Ethernet1/1/1  N9K-
C9336C-FX2

node2      /cdp
            e0a    cs1                       Ethernet1/2    N5K-
C5596UP
            e0b    cs2-new                   Ethernet1/1/2  N9K-
C9336C-FX2
```

Verifique se as portas do cluster movidas veem o switch CS2-novo como vizinho.

13. Confirme as conexões da porta do switch a partir da perspetiva do switch CS2-novo:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. No switch de cluster CS1, encerre as portas conetadas às portas de cluster de **todos** os nós para fazer failover dos LIFs de cluster.

```
cs1# configure
cs1(config)# interface eth1/1-1/2
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
```

Todas as LIFs de cluster fazem failover para o switch de CS2 novos.

15. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch CS2-novo. Isso pode levar alguns segundos:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interfac     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.3.4/16     node1
e0b     false
            node1_clus2  up/up      169.254.3.5/16     node1
e0b     true
            node2_clus1  up/up      169.254.3.8/16     node2
e0b     false
            node2_clus2  up/up      169.254.3.9/16     node2
e0b     true
```

16. Verifique se o cluster está em bom estado:

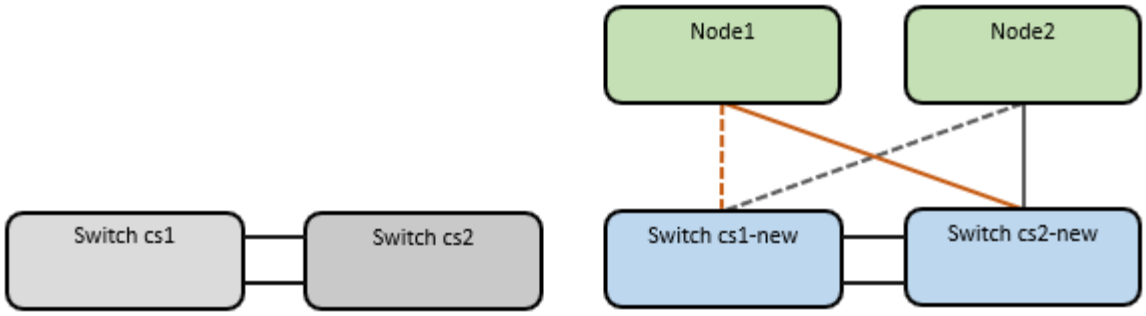
    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

17. Mova os cabos de conexão do nó do cluster de CS1 para o novo switch de CS1 novos.

    Os cabos de conexão do nó de cluster foram movidos para o switch de CS1 novo



18. Confirme a integridade das conexões de rede movidas para CS1-new:

    `network port show -ipspace Cluster`

    Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Todas as portas de cluster que foram movidas devem estar para cima.

19. Verifique as informações do vizinho nas portas do cluster:

    `network device-discovery show`

    Mostrar exemplo

    ```
    cluster1::*> network device-discovery show -protocol cdp
    Node/       Local  Discovered
    Protocol    Port   Device (LLDP: ChassisID)  Interface
    Platform
    ----------- ------ ------------------------- --------------
    --------------
    node1      /cdp
                e0a    cs1-new                   Ethernet1/1/1   N9K-
    C9336C-FX2
                e0b    cs2-new                   Ethernet1/1/2   N9K-
    C9336C-FX2

    node2      /cdp
                e0a    cs1-new                   Ethernet1/1/1   N9K-
    C9336C-FX2
                e0b    cs2-new                   Ethernet1/1/2   N9K-
    C9336C-FX2
    ```

    Verifique se as portas do cluster movidas veem o switch CS1-novo como vizinho.

20. Confirme as conexões da porta do switch a partir da perspetiva do switch CS1-novo:

    ```
    cs1-new# show interface brief
    cs1-new# show cdp neighbors
    ```

21. Verifique se o ISL entre CS1-novo e CS2-novo ainda está operacional:

    `show port-channel summary`

Mostrar exemplo

```
cs1-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

cs2-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

Etapa 3: Verifique a configuração

1. Ative a reversão automática nos LIFs do cluster.

   `network interface modify -vserver Cluster -lif * -auto-revert true`

2. Verifique se os LIFs de cluster reverteram para suas portas residenciais (isso pode levar um minuto):

   `network interface show -vserver Cluster`

Se os LIFs de cluster não tiverem revertido para sua porta inicial, reverta-os manualmente:

```
network interface revert -vserver Cluster -lif *
```

3. Verifique se o cluster está em bom estado:

```
cluster show
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:...
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=END`

O que se segue?

Depois de migrar os switches, você"configurar monitoramento de integridade do switch" .

Migrar para cluster comutado de dois nós

Se você tiver um ambiente de cluster *sem switch* de dois nós existente, poderá migrar para um ambiente de cluster *com switch* de dois nós usando os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

O processo de migração funciona para todos os nós que usam portas óticas ou Twinax, mas não é suportado neste switch se os nós estiverem usando portas integradas 10Gb BASE-T RJ45 para as portas de cluster-rede.

Rever os requisitos

O que você vai precisar

- Para a configuração sem switch de dois nós:
  - A configuração sem switch de dois nós está corretamente configurada e funcionando.

- Todas as portas de cluster estão no estado **up**.
- Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e em suas portas domésticas.
- Consulte "Hardware Universe" para obter todas as versões suportadas do ONTAP.

- Para a configuração do switch Cisco Nexus 9336C-FX2:
  - Ambos os switches têm conetividade de rede de gerenciamento.
  - Existe acesso à consola aos interrutores do cluster.
  - As conexões de switch de nó para nó Nexus 9336C-FX2 e switch para switch usam cabos Twinax ou fibra.

    Consulte "Hardware Universe" para obter mais informações sobre cabeamento.
- Os cabos ISL (Inter-Switch Link) são conetados às portas 1/35 e 1/36 em ambos os switches 9336C-FX2.
- A personalização inicial de ambos os switches 9336C-FX2 está concluída, de modo que:
  - Os switches 9336C-FX2 estão executando a versão mais recente do software.
  - Os arquivos de configuração de referência (RCFs) são aplicados aos switches. Qualquer personalização de site, como SMTP, SNMP e SSH, é configurada nos novos switches.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches 9336C-FX2 são CS1 e CS2.
- Os nomes dos SVMs do cluster são node1 e node2.
- Os nomes dos LIFs são node1_clus1 e node1_clus2 no nó 1 e node2_clus1 e node2_clus2 no nó 2 respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas do cluster usadas neste procedimento são e0a e e0b.

```
https://hwu.netapp.com["Hardware Universe"^]Consulte para obter
informações sobre as portas de cluster para as suas plataformas.
```

Migrar os switches

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

Etapa 2: Configurar portas e cabeamento

1. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster CS1 e CS2.

   Não desative as portas ISL.

   Mostrar exemplo

   O exemplo a seguir mostra que as portas 1 a 34 voltadas para o nó estão desativadas no switch CS1:

   ```
   cs1# config
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
   e1/5/1-4, e1/6/1-4, e1/7-34
   cs1(config-if-range)# shutdown
   ```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches 9336C-FX2 CS1 e CS2 estão acima nas portas 1/35 e 1/36:

   ```
   show port-channel summary
   ```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS1:

```
cs1# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS2:

```
(cs2)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

3. Exibir a lista de dispositivos vizinhos:

`show cdp neighbors`

Este comando fornece informações sobre os dispositivos que estão conetados ao sistema.

Mostrar exemplo

O exemplo a seguir lista os dispositivos vizinhos no switch CS1:

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 2
```

O exemplo a seguir lista os dispositivos vizinhos no switch CS2:

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1                Eth1/35        177    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        177    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 2
```

4. Verifique se todas as portas do cluster estão ativas:

   `network port show -ipspace Cluster`

   Cada porta deve ser exibida para `Link` e saudável para `Health Status`.

   Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node2

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

5. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show -vserver Cluster`

   Cada LIF de cluster deve ser exibido `true Is Home` e ter um `Status Admin/Oper` de up/up.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

   `network interface show -vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. Desconete o cabo da porta de cluster e0a no node1 e conete o e0a à porta 1 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.

O "Hardware Universe - interrutores" contém mais informações sobre cabeamento.

"Hardware Universe - interrutores"

8. Desconete o cabo da porta de cluster e0a no node2 e conete o e0a à porta 2 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
9. Habilite todas as portas voltadas para o nó no switch de cluster CS1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão ativadas no switch CS1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# no shutdown
```

10. Verifique se todas as LIFs do cluster estão ativas, operacionais e exibidas como `true` para `Is Home`:

```
network interface show -vserver Cluster
```

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> network interface show -vserver Cluster

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node         Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1        e0a
true
         node1_clus2  up/up      169.254.49.125/16  node1        e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2        e0a
true
         node2_clus2  up/up      169.254.19.183/16  node2        e0b
true

4 entries were displayed.
```

11. Exibir informações sobre o status dos nós no cluster:

    `cluster show`

Mostrar exemplo

O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false

2 entries were displayed.
```

12. Desconete o cabo da porta de cluster e0b no node1 e conete o e0b à porta 1 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.

13. Desconete o cabo da porta de cluster e0b no node2 e conete o e0b à porta 2 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
14. Habilite todas as portas voltadas para o nó no switch de cluster CS2.

    Mostrar exemplo

    O exemplo a seguir mostra que as portas 1/1 a 1/34 estão ativadas no switch CS2:

    ```
    cs2# config
    Enter configuration commands, one per line. End with CNTL/Z.
    cs2(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
    e1/5/1-4, e1/6/1-4, e1/7-34
    cs2(config-if-range)# no shutdown
    ```

15. Verifique se todas as portas do cluster estão ativas:

    ```
    network port show -ipspace Cluster
    ```

Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão em node1 e node2:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.
```

Etapa 3: Verifique a configuração

1. Verifique se todas as interfaces exibem verdadeiro para `Is Home`:

   `network interface show -vserver Cluster`

   Isso pode levar vários minutos para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> network interface show -vserver Cluster

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true

4 entries were displayed.
```

2. Verifique se ambos os nós têm uma conexão com cada switch:

   `show cdp neighbors`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
(cs1)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4

(cs2)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0b
node2              Eth1/2         133    H           FAS2980
e0b
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Exiba informações sobre os dispositivos de rede descobertos no cluster:

   `network device-discovery show -protocol cdp`

   Mostrar exemplo

   ```
   cluster1::*> network device-discovery show -protocol cdp
   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID)  Interface
   Platform
   ----------- ------ ------------------------- ----------------
   ----------------
   node2      /cdp
               e0a    cs1                       0/2               N9K-
   C9336C
               e0b    cs2                       0/2               N9K-
   C9336C
   node1      /cdp
               e0a    cs1                       0/1               N9K-
   C9336C
               e0b    cs2                       0/1               N9K-
   C9336C

   4 entries were displayed.
   ```

4. Verifique se as definições estão desativadas:

   `network options switchless-cluster show`

   > Pode demorar vários minutos para o comando ser concluído. Aguarde até que o anúncio "3 minutos de duração expire".

   Mostrar exemplo

   A saída falsa no exemplo a seguir mostra que as configurações estão desativadas:

   ```
   cluster1::*> network options switchless-cluster show
   Enable Switchless Cluster: false
   ```

5. Verifique o status dos membros do nó no cluster:

   `cluster show`

Mostrar exemplo

O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

Depois de migrar seus switches, você"configurar monitoramento de integridade do switch" .

Substitua os interruptores

Substituir switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Siga estas etapas para substituir switches Nexus 9336C-FX2 e 9336C-FX2-T defeituosos em uma rede de cluster. Este é um procedimento não disruptivo (NDU).

Rever os requisitos

Antes de efetuar a substituição do interrutor, certifique-se de que:

- Você verificou o número de série do switch para garantir que o switch correto seja substituído.
- No cluster existente e na infra-estrutura de rede:
  - O cluster existente é verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
  - Todas as portas de cluster são **up**.
  - Todas as interfaces lógicas de cluster (LIFs) são **up** e em suas portas domésticas.
  - O comando ONTAP `cluster ping-cluster -node node1` deve indicar que a conetividade básica e a comunicação maior do que a PMTU são bem-sucedidas em todos os caminhos.
- No interrutor de substituição do Nexus 9336C-FX2:
  - A conetividade de rede de gerenciamento no switch de substituição está funcional.
  - O acesso do console ao interrutor de substituição está no lugar.
  - As conexões de nó são as portas 1/1 a 1/34.
  - Todas as portas ISL (Inter-Switch Link) estão desativadas nas portas 1/35 e 1/36.
  - O arquivo de configuração de referência desejado (RCF) e o interrutor de imagem do sistema operacional NX-os são carregados no switch.
  - A personalização inicial do interrutor está completa, como detalhado em "Configure o interrutor do cluster 9336C-FX2".

    Quaisquer personalizações de sites anteriores, como STP, SNMP e SSH, são copiadas para o novo switch.
- Você executou o comando para migrar um LIF de cluster do nó onde o LIF de cluster está hospedado.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desativar a criação de casos durante a manutenção. Consulte este artigo da base de dados de Conhecimento "SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para obter mais detalhes.
- Ativar o registo de sessão para quaisquer sessões CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" neste artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Substitua o interrutor

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches Nexus 9336C-FX2 existentes são CS1 e CS2.
- O nome do novo switch Nexus 9336C-FX2 é newcs2.
- Os nomes dos nós são node1 e node2.
- As portas de cluster em cada nó são denominadas e0a e e0b.
- Os nomes de LIF do cluster são node1_clus1 e node1_clus2 para node1, e node2_clus1 e node2_clus2

para node2.

- O prompt para alterações em todos os nós de cluster é cluster1::*>

Sobre esta tarefa

O procedimento a seguir é baseado na seguinte topologia de rede de cluster:

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
4 entries were displayed.



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C
4 entries were displayed.



cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2                Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
cs2(FDO220329V5)   Eth1/36        176    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1                Eth1/35        178    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        178    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

Passo 1: Prepare-se para a substituição

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Instale o RCF e a imagem apropriados no interrutor, newcs2, e faça os preparativos necessários para o local.

   Se necessário, verifique, baixe e instale as versões apropriadas do software RCF e NX-os para o novo switch. Se tiver verificado que o novo switch está corretamente configurado e não precisa de atualizações para o software RCF e NX-os, avance para o passo 2.

   a. Vá para a página *NetApp Cluster and Management Network switches Referência Configuração do arquivo Descrição* no site de suporte da NetApp.
   b. Clique no link para a *Cluster Network and Management Network Compatibility Matrix* e observe a versão necessária do software do switch.
   c. Clique na seta de volta do navegador para retornar à página Descrição, clique em **CONTINUAR**, aceite o contrato de licença e vá para a página Download.
   d. Siga as etapas na página Download para baixar os arquivos RCF e NX-os corretos para a versão do software ONTAP que você está instalando.

3. No novo switch, faça login como administrador e encerre todas as portas que serão conetadas às interfaces do cluster de nós (portas 1/1 a 1/34).

Se o interrutor que está a substituir não estiver funcional e estiver desligado, avance para o passo 4. As LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

Mostrar exemplo

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-34
newcs2(config-if-range)# shutdown
```

4. Verifique se todas as LIFs do cluster têm a reversão automática ativada:

   `network interface show -vserver Cluster -fields auto-revert`

   Mostrar exemplo

```
cluster1::> network interface show -vserver Cluster -fields auto-
revert

             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Etapa 2: Configurar cabos e portas

1. Desligue as portas ISL 1/35 e 1/36 no switch Nexus 9336C-FX2 CS1.

   Mostrar exemplo

   ```
   cs1# configure
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/35-36
   cs1(config-if-range)# shutdown
   cs1(config-if-range)#
   ```

2. Remova todos os cabos do switch Nexus 9336C-FX2 CS2 e conete-os às mesmas portas do switch Nexus C9336C-FX2 newcs2.
3. Abra as portas ISLs 1/35 e 1/36 entre os switches CS1 e newcs2 e verifique o status da operação do canal da porta.

   O Canal de porta deve indicar PO1(SU) e os portos Membros devem indicar eth1/35(P) e eth1/36(P).

Mostrar exemplo

Este exemplo ativa as portas ISL 1/35 e 1/36 e apresenta o resumo do canal da porta no interrutor CS1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/35-36
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member       Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

cs1(config-if-range)#
```

4. Verifique se a porta e0b está ativa em todos os nós:

   `network port show ipspace Cluster`

Mostrar exemplo

A saída deve ser semelhante ao seguinte:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/auto   -
false

4 entries were displayed.
```

5. No mesmo nó usado na etapa anterior, reverta o LIF do cluster associado à porta na etapa anterior usando o comando de reversão da interface de rede.

Mostrar exemplo

Neste exemplo, LIF node1_clus2 no node1 é revertido com sucesso se o valor Casa for verdadeiro e a porta for e0b.

Os comandos a seguir retornam LIF `node1_clus2` `node1` à porta inicial `e0a` e exibem informações sobre os LIFs em ambos os nós. Abrir o primeiro nó é bem-sucedido se a coluna is Home for verdadeira para ambas as interfaces de cluster e elas mostrarem as atribuições de porta corretas, neste `e0a` exemplo e `e0b` no node1.

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Exibir informações sobre os nós em um cluster:

`cluster show`

Mostrar exemplo

Este exemplo mostra que a integridade do nó para node1 e node2 neste cluster é verdadeira:

```
cluster1::*> cluster show

Node          Health  Eligibility
------------- ------- ------------
node1         false   true
node2         true    true
```

7. Verifique se todas as portas de cluster físico estão ativas:

   `network port show ipspace Cluster`

   Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node node1
Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e0a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e0b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e0a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up    9000  auto/10000
healthy  false

4 entries were displayed.
```

8. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Etapa 3: Verifique a configuração

1. Confirme a seguinte configuração de rede de cluster:

   ```
   network port show
   ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster
Node: node1

Ignore
                                        Speed(Mbps)            Health
Health
Port      IPspace     Broadcast Domain Link MTU   Admin/Oper  Status
Status
--------- ----------- ---------------- ---- ----- -----------
-------- ------
e0a       Cluster     Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster     Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                         Speed(Mbps)           Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000 auto/10000
healthy  false

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

cluster1::> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C9336C
            e0b    newcs2                    0/2               N9K-
C9336C
node1      /cdp
            e0a    cs1                       0/1               N9K-
C9336C
            e0b    newcs2                    0/1               N9K-
C9336C

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2               Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
newcs2               Eth1/36        176    R S I s     N9K-C9336C
```

```
Eth1/36

Total entries displayed: 4


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e0b
node2              Eth1/2         124    H           FAS2980
e0b
cs1                Eth1/35        178    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        178    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

Depois de substituir seus interruptores, você"configurar monitoramento de integridade do switch" .

Substituir os switches de cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.

- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

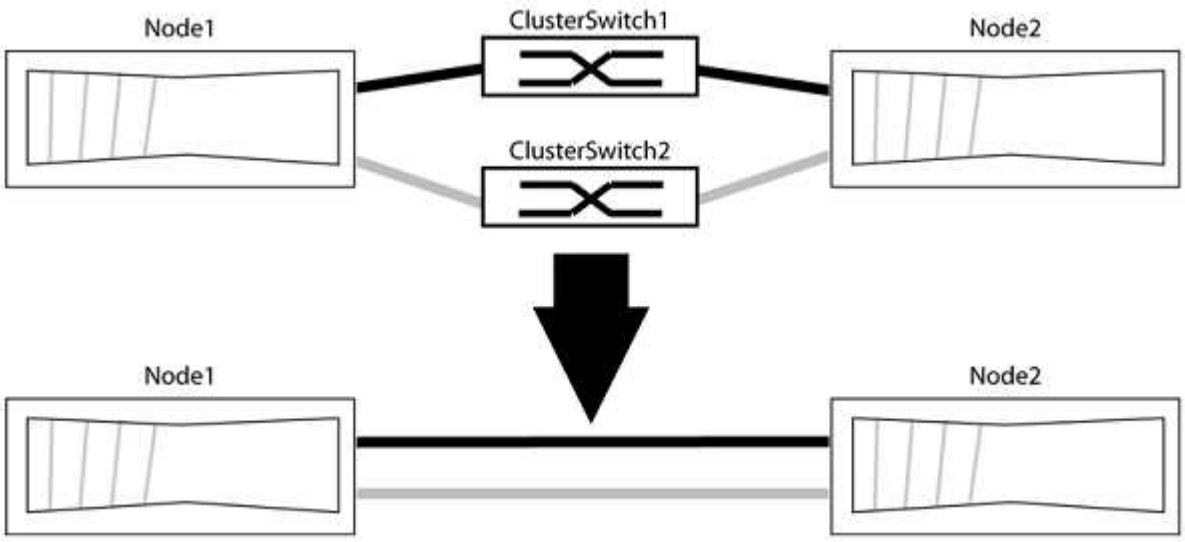
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

`network options detect-switchless-cluster show`

Mostrar exemplo

A saída de exemplo a seguir mostra se a opção está ativada.

```
cluster::*> network options detect-switchless-cluster show
   (network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

`system node autosupport invoke -node * -type all -message MAINT=<number_of_hours>h`

`h`onde está a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico desta tarefa de manutenção para que possa suprimir a criação automática de casos durante a janela de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

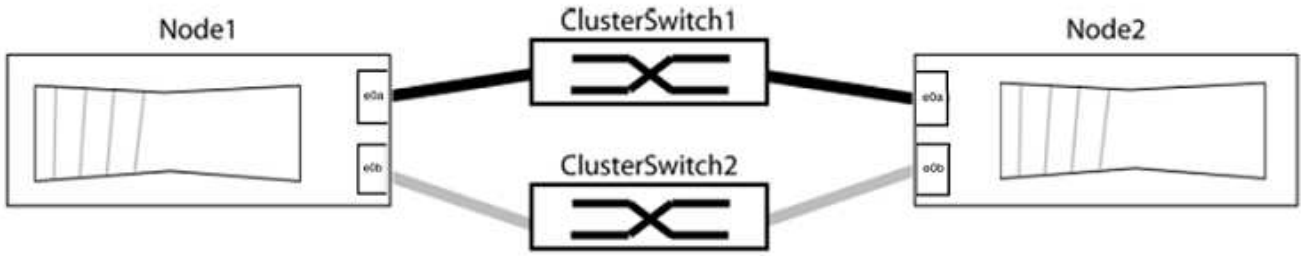
Mostrar exemplo

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-cisco-9336c-fx2/+ `network port show -ipspace Cluster`

No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

`network interface show -vserver Cluster -fields is-home`

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

`network interface revert -vserver Cluster -lif *`

4. Desativar a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert false`

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

   `network device-discovery show -port` *`cluster_port`*

   A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

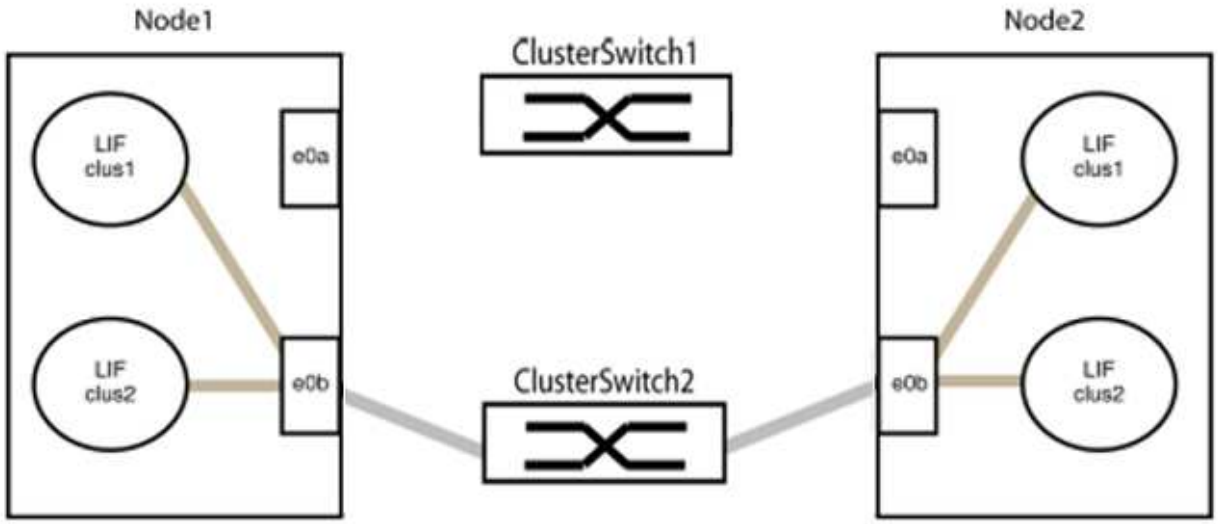
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   > Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

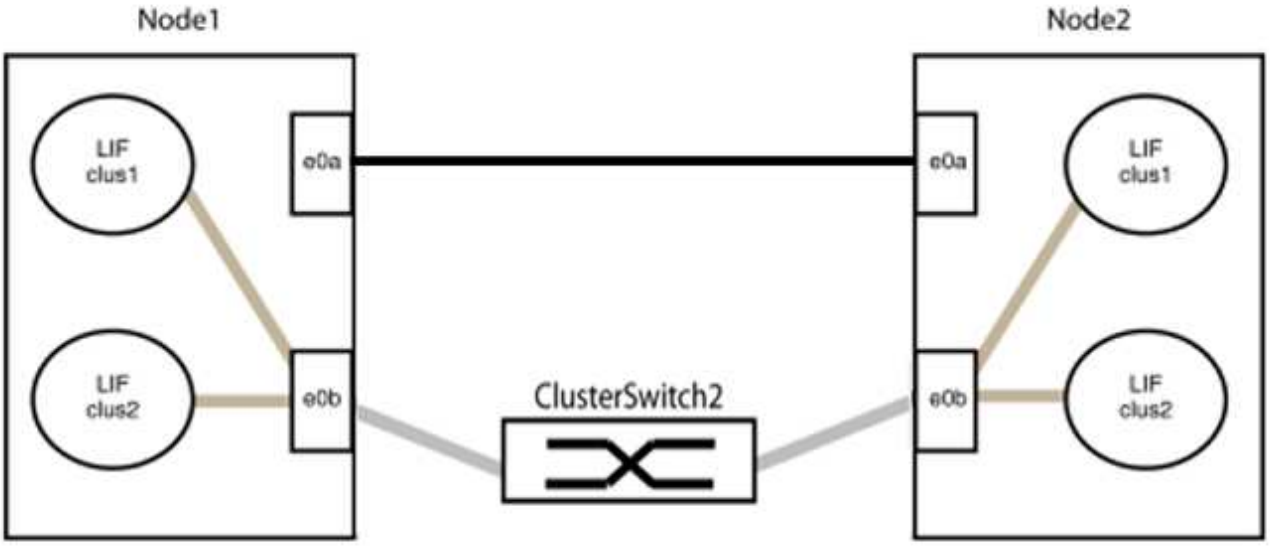
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

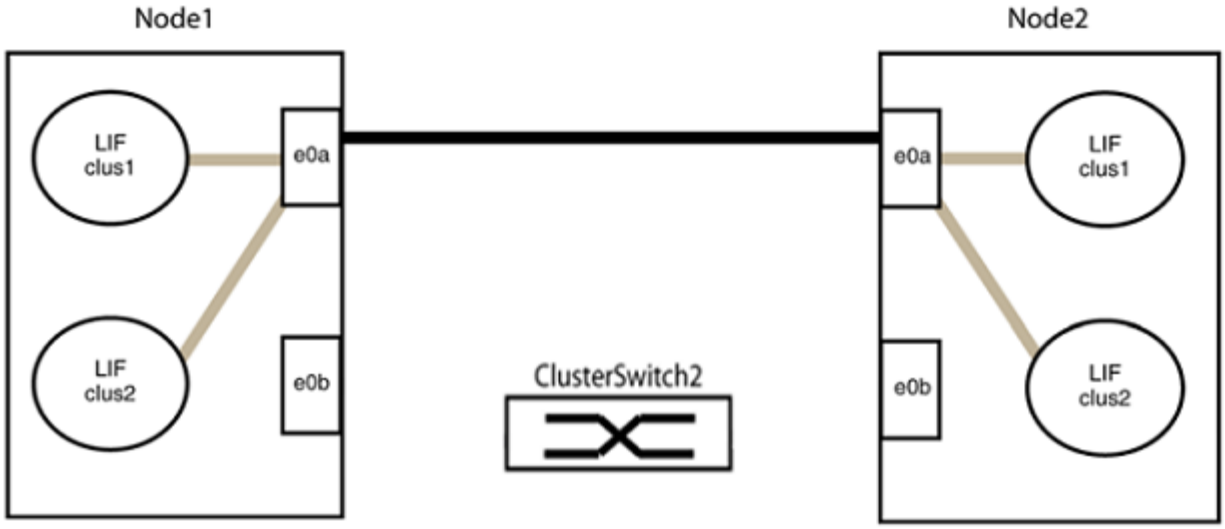
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

   No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

   `network device-discovery show -port cluster_port`

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

NVIDIA SN2100

Comece agora

Fluxo de trabalho de instalação e configuração para switches NVIDIA SN2100

O NVIDIA SN2100 é um switch de cluster que permite criar clusters do ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches NVIDIA SN2100.

1 **"Revise os requisitos de configuração"**

Revise os requisitos de configuração para o switch de cluster SN2100.

2 **"Revise os componentes e números de peça"**

Revise os componentes e números de peça do switch de cluster SN2100.

3 **"Revise a documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches SN2100 e o cluster ONTAP .

4 **"Instale o hardware"**

Instale o hardware do switch.

5 **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar todos os requisitos de configuração.

Requisitos de instalação

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar switches de gerenciamento adicionais, que são opcionais.

Você instala o switch NVIDIA SN2100 (X190006) no gabinete de switch duplo/único NVIDIA com os suportes padrão incluídos no switch.

Para obter diretrizes de cabeamento, "Analise as considerações sobre cabeamento e configuração"consulte .

Suporte a ONTAP e Linux

O switch NVIDIA SN2100 é um switch 10/25/40/100GbE que executa o Cumulus Linux. O interrutor suporta o seguinte:

- ONTAP 9.10.1P3 e posterior

  O switch SN2100 serve aplicativos de cluster e armazenamento no ONTAP 9.10.1P3 e posterior em diferentes pares de switches.

- Versões do SO Cumulus Linux (CL)
  - As versões específicas do CL são qualificadas e suportadas pelo NetApp. Para obter informações de compatibilidade atuais, consulte a "Informações sobre switches Ethernet NVIDIA" página ou o "NetApp

Hardware Universe".

- Para fazer o download do software Cumulus SN2100 da NVIDIA, você deve ter credenciais de login para acessar o Portal de suporte Empresarial da NVIDIA. Consulte o artigo da base de dados de Conhecimento "Como se Registrar no NVIDIA para acesso ao Portal de suporte Empresarial" .

- Você pode instalar o Cumulus Linux quando o switch estiver executando Cumulus Linux ou ONIE.

O que se segue?

"Componentes e números de peça" .

Componentes e números de peça para interrutores NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar a lista de componentes e números de peça do kit de gabinete e trilho.

Detalhes do gabinete

Você instala o switch NVIDIA SN2100 (X190006) no gabinete de switch duplo/único NVIDIA com os suportes padrão incluídos no switch.

Detalhes do kit de calha

A tabela a seguir lista o número de peça e a descrição dos SN2100 interrutores e kits de trilho:

Número de peça	Descrição
X190006-PE	Interrutor de cluster, NVIDIA SN2100, 16pt 100GbE, PTSX
X190006-PI	Comutador de cluster, NVIDIA SN2100, 16pt 100GbE, PSIN
X-MTEF-KIT-D	Kit de calha, interrutor duplo NVIDIA lado a lado
X-MTEF-KIT-E	Kit de calha, NVIDIA interrutor simples, profundidade curta

Consulte a documentação do NVIDIA para obter detalhes "Instalar o seu kit de comutador e calha SN2100" sobre .

O que se segue?

"Documentação necessária" .

Requisitos de documentação para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar toda a documentação recomendada.

Título	Descrição
"Guia de instalação do interrutor NVIDIA"	Descreve como instalar seus switches NVIDIA SN2100.

Título	Descrição
"Guia de cabeamento de compartimento de unidade NVMe de NS224 GB"	Visão geral e ilustrações mostrando como configurar o cabeamento para compartimentos de unidades.
"NetApp Hardware Universe"	Permite confirmar o hardware suportado, como switches de armazenamento e cabos, para o modelo da sua plataforma.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches NVIDIA SN2100

Para instalar e configurar o hardware de um switch de cluster SN2100, siga estas etapas:

1. **"Instale o hardware"**

Instale o hardware do switch.

2. **"Analise as considerações sobre cabeamento e configuração"**

Revise os requisitos para conexões óticas, o adaptador QSA e a velocidade do switchport.

3. **"Cable as NS224 prateleiras"**

Siga os procedimentos de cabeamento se você tiver um sistema no qual os NS224 compartimentos de unidades precisam ser cabeados como storage conectado a switch (não storage com conexão direta).

Instale o hardware do switch NVIDIA SN2100

Para instalar o hardware SN2100, consulte a documentação do NVIDIA.

Passos

1. Reveja o "requisitos de configuração".
2. Siga as instruções em "Guia de instalação do interrutor NVIDIA".

O que se segue?

"Revise o cabeamento e a configuração" .

Analise as considerações sobre cabeamento e configuração

Antes de configurar o switch NVIDIA SN2100, revise as seguintes considerações.

Detalhes da porta NVIDIA

Portas de comutação	* Uso de portas*

swp1s0-3	4x10GbE breakout cluster port Nodes
swp2s0-3	4x25GbE breakout cluster port Nodes
swp3-14	Nós de porta de cluster 40/100GbE
swp15-16	100GbE portas ISL (Inter-Switch Link)

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Atrasos de ligação com ligações óticas

Se você estiver enfrentando atrasos de link-up de mais de cinco segundos, o Cumulus Linux 5,4 e posterior inclui suporte para link-up rápido. Você pode configurar os links usando o `nv set` comando da seguinte forma:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Mostrar exemplo

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Suporte para conexões de cobre

As seguintes alterações de configuração são necessárias para corrigir esse problema.

Cumulus Linux 4.4.3

1. Identifique o nome de cada interface usando cabos de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Adicione as duas linhas a seguir ao `/etc/cumulus/switchd.conf` arquivo para cada porta (swp<n>) que esteja usando cabos de cobre 40GbE/100GbE:

   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   Por exemplo:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Reinicie `switchd` o serviço:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirme se as portas estão ativas:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
```

Cumulus Linux 5.x

1. Identifique o nome de cada interface usando cabos de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface --view=pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Configure os links usando o `nv set` comando da seguinte forma:
   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Recarregue o `switchd` serviço

     Por exemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Confirme se as portas estão ativas:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode        LLDP                Summary
-----  --------- ----  -----  ----------  ------------------  --------
UP     swp3      100G  9216   Trunk/L2                        Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                        Master:
bridge(UP)
```

Consulte o artigo da base de dados de Conhecimento "O switch SN2100 não consegue se conetar usando cabos de cobre 40/100GbE" para obter mais detalhes.

No Cumulus Linux 4,4.2, as conexões de cobre não são suportadas em switches SN2100 com X1151A portas NIC, X1146A NIC ou 100GbE integradas. Por exemplo:

- AFF A800 nas portas e0a e e0b
- AFF A320 nas portas e0g e e0h

Adaptador QSA

Quando um adaptador QSA é usado para se conetar às portas de cluster 10GbE/25GbE em uma plataforma, o link pode não aparecer.

Para resolver esse problema, faça o seguinte:

- Para 10GbE, defina manualmente a velocidade do link swp1s0-3 para 10000 e defina a negociação automática como desativada.
- Para 25GbE, defina manualmente a velocidade do link swp2s0-3 para 25000 e defina a negociação automática como desativada.

Ao usar adaptadores QSA 10GbE/25GbE, insira-os em portas 40GbE/100GbE não-breakout (swp3-swp14). Não insira o adaptador QSA em uma porta configurada para breakout.

Definição da velocidade da interface nas portas de arranque

Dependendo do transcetor na porta do switch, talvez seja necessário definir a velocidade na interface do switch para uma velocidade fixa. Se estiver usando portas multiconexões 10GbE e 25GbE, verifique se a negociação automática está desligada e defina a velocidade da interface no switch.

Cumulus Linux 4.4.3

Por exemplo:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces     2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000  <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
     alias 10G Intra-Cluster Node
-    link-autoneg off
+    link-autoneg on
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp2s0
iface swp2s0
     alias 25G Intra-Cluster Node
     link-autoneg off
     link-speed 25000 <---- port speed set
```

Verifique a interface e o status da porta para verificar se as configurações são aplicadas:

```
cumulus@cumulus:mgmt:~$ net show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Cumulus Linux 5.x

Por exemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate        off                   off
off
  duplex                full                  full
full
  speed                 10G                   10G
10G
  fec                   auto                  auto
auto
  mtu                   9216                  9216
9216
[breakout]

  state                 up                    up
up
```

Verifique a interface e o status da porta para verificar se as configurações são aplicadas:

```
cumulus@cumulus:mgmt:~$ nv show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

O que se segue?

"Cabo NS224 prateleiras como storage conetado a switch".

Prenda as NS224 gavetas como storage conetado a switch

Se você tiver um sistema no qual os NS224 compartimentos de unidades precisem ser cabeados como storage conectado ao switch (não storage com conexão direta), use as informações fornecidas aqui.

- Cabos NS224 shelves de unidade através de switches de armazenamento:

  "Cabeamento de compartimentos de unidades NS224 conectados a switch"

- Confirme o hardware suportado, como switches de armazenamento e cabos, para o modelo da sua plataforma:

  "NetApp Hardware Universe"

O que se segue?

"Configure o interrutor".

Configurar o software

Fluxo de trabalho de instalação de software para switches NVIDIA SN2100

Para instalar e configurar o software para um switch NVIDIA SN2100, siga estas etapas:

1. **"Configure o interrutor"**

   Configurar o switch NVIDIA SN2100.

2. **"Instale o Cumulus Linux no modo Cumulus"**

   Você pode instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver executando o Cumulus Linux.

3. **"Instale o Cumulus Linux no modo ONIE"**

   Como alternativa, você pode instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver executando o Cumulus Linux no modo ONIE.

4. **"Atualize sua versão do Cumulus Linux, conforme necessário"**

   Você pode atualizar seu sistema operacional Cumulus Linux (CL) conforme necessário.

5. **"Instale ou atualize o script RCF (Reference Configuration File)"**

   Existem dois scripts RCF disponíveis para aplicativos de agrupamento e armazenamento. O procedimento para cada um é o mesmo.

6. **"Instale o arquivo CSHM"**

   Você pode instalar o arquivo de configuração aplicável para o monitoramento de integridade do switch Ethernet dos switches de cluster NVIDIA.

7 **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações do switch do cluster SN2100.

Configure o switch NVIDIA SN2100

Para configurar o switch SN2100, consulte a documentação do NVIDIA.

Passos

1. Reveja o "requisitos de configuração".
2. Siga as instruções em "Apresentação do sistema NVIDIA.".

O que se segue?

"Instale o Cumulus Linux no modo Cumulus"ou"Instale o Cumulus Linux no modo ONIE" .

Instale o Cumulus Linux no modo Cumulus

Siga este procedimento para instalar o SO Cumulus Linux (CL) quando o switch estiver em execução no modo Cumulus.

O SO Cumulus Linux (CL) pode ser instalado quando o switch está executando o Cumulus Linux ou ONIE ("Instale no modo ONIE"consulte).

Antes de começar

Certifique-se de que tem o seguinte:

- Conhecimento do Linux de nível intermediário.
- Familiaridade com edição de texto básica, permissões de arquivo UNIX e monitoramento de processos. Uma variedade de editores de texto são pré-instalados, `vi` incluindo e `nano`.
- Acesso a um shell Linux ou UNIX. Se você estiver executando o Windows, use um ambiente Linux como sua ferramenta de linha de comando para interagir com o Cumulus Linux.
- O requisito de taxa de transmissão é definido como 115200 no switch de console serial para acesso ao console de switch NVIDIA SN2100, como segue:
  - 115200 baud
  - 8 bits de dados
  - 1 bit de paragem
  - paridade: nenhuma
  - controle de fluxo: nenhum

Sobre esta tarefa

Tenha em atenção o seguinte:

Cada vez que o Cumulus Linux é instalado, toda a estrutura do sistema de arquivos é apagada e reconstruída.

A senha padrão para a conta de usuário do Cumulus é **Cumulus**. A primeira vez que você fizer login no Cumulus Linux, você deve alterar essa senha padrão. Certifique-se de atualizar quaisquer scripts de automação antes de instalar uma nova imagem. O Cumulus Linux fornece opções de linha de comando para alterar a senha padrão automaticamente durante o processo de instalação.

Exemplo 1. Passos

Cumulus Linux 4.4.3

1. Inicie sessão no interrutor.

   O login pela primeira vez no switch requer nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo` o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

   Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina a data, a hora, o fuso horário e o servidor NTP no switch.
   a. Verifique o fuso horário atual:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Atualizar para o novo fuso horário:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

d. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

i. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Instale o Cumulus Linux 4,4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 4,4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

Cumulus Linux 5.4.0

1. Inicie sessão no interrutor.

   O login pela primeira vez no switch requer nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo`

o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

> Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

> Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina o fuso horário, a data, a hora e o servidor NTP no switch.
   a. Defina o fuso horário:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

   c. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

   d. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Veja o artigo da Base de Conhecimento "A configuração do servidor NTP não está funcionando com os switches NVIDIA SN2100" para mais detalhes.

g. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale o Cumulus Linux 5,4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 5,4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational          applied              description
-------------------- -------------------- --------------------
hostname             cumulus              cumulus
build                Cumulus Linux 5.4.0  system build version
uptime               6 days, 13:37:36     system uptime
timezone             Etc/UTC              system time zone
```

11. Verifique se os nós têm uma conexão com cada switch:

```
cumulus@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   Mgmt        mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

12. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Adicione grupos de usuários adicionais para que o usuário admin acesse `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user 'admin' to group 'nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

Cumulus Linux 5.11.0

1. Inicie sessão no interrutor.

   Quando você faz login no switch pela primeira vez, ele requer o nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo` o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

   Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

   Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina o fuso horário, a data, a hora e o servidor NTP no switch.
   a. Defina o fuso horário:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

   c. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Veja o artigo da Base de Conhecimento "A configuração do servidor NTP não está funcionando com os switches NVIDIA SN2100" para mais detalhes.

g. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale o Cumulus Linux 5,11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 5,11.0:

    `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied                 description
------------------- ----------------------- --------------------
build               Cumulus Linux 5.11.0
uptime              153 days, 2:44:16
hostname            cumulus                 cumulus
product-name        Cumulus Linux
product-release     5.11.0
platform            x86_64-mlnx_x86-r0
system-memory       2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory         0 Bytes used / 0 Bytes free / 0 Bytes total
health-status       not OK
date-time           2025-04-23 09:55:24
status              N/A
timezone            Etc/UTC
maintenance
  mode              disabled
  ports             enabled
version
  kernel            6.1.0-cl-1-amd64
  build-date        Thu Nov 14 13:06:38 UTC 2024
  image             5.11.0
  onie              2019.11-5.2.0020-115200
```

11. Verifique se cada nó tem uma conexão com cada switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   eth   mgmt-sw1
Eth110/1/14
swp2s1     25G    Trunk/L2    node1
e0a
swp1s1     10G    swp   sw2
e0a
swp9       100G   swp   sw3
e4a
swp10      100G   swp   sw4
e4a
swp15      100G   swp   sw5
swp15
swp16      100G   swp   sw6
swp16
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

O que se segue?

"Instale o script RCF (Reference Configuration File)".

Instale o Cumulus Linux no modo ONIE

Siga este procedimento para instalar o SO Cumulus Linux (CL) quando o switch estiver em execução no modo ONIE.

> O SO Cumulus Linux (CL) pode ser instalado quando o switch está executando ONIE ou Cumulus Linux ("Instale no modo Cumulus"consulte).

Sobre esta tarefa

Você pode instalar o Cumulus Linux usando o Open Network Install Environment (ONIE) que permite a descoberta automática de uma imagem do instalador de rede. Isso facilita o modelo de sistema de proteção de switches com uma escolha de sistema operacional, como o Cumulus Linux. A maneira mais fácil de instalar o Cumulus Linux com ONIE é com descoberta HTTP local.

> Se o seu host estiver habilitado para IPv6, verifique se ele está executando um servidor da Web. Se o seu host estiver habilitado para IPv4, verifique se ele está executando o DHCP além de um servidor da Web.

Este procedimento demonstra como atualizar o Cumulus Linux após o administrador ter inicializado no ONIE.

Exemplo 2. Passos

Cumulus Linux 4.4.3

1. Baixe o arquivo de instalação Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo para: `onie-installer`.
2. Conete o host à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interrutor.

   O switch faz o download do instalador de imagem ONIE e inicializa. Após a conclusão da instalação, o prompt de login do Cumulus Linux aparece na janela do terminal.

   > Cada vez que o Cumulus Linux é instalado, toda a estrutura do sistema de arquivos é apagada e reconstruída.

4. Reinicie o switch SN2100:

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

5. Pressione a tecla **ESC** na tela GNU GRUB para interromper o processo de inicialização normal, selecione **ONIE** e pressione **Enter**.
6. Na próxima tela, selecione **ONIE: Install os**.
7. O processo de descoberta do instalador ONIE é executado procurando a instalação automática. Pressione **Enter** para interromper temporariamente o processo.
8. Quando o processo de descoberta for interrompido:

   ```
   ONIE:/ # onie-stop
   discover: installer mode detected.
   Stopping: discover...start-stop-daemon: warning: killing process
   427:
   No such process done.
   ```

9. Se o serviço DHCP estiver em execução na rede, verifique se o endereço IP, a máscara de sub-rede e o gateway padrão estão corretamente atribuídos:

   ```
   ifconfig eth0
   ```

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.233.204.1    0.0.0.0         UG    0      0
0   eth0
10.233.204.0    *               255.255.254.0   U     0      0
0   eth0
```

10. Se o esquema de endereçamento IP for definido manualmente, faça o seguinte:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Repita o passo 9 para verificar se as informações estáticas foram introduzidas corretamente.
12. Instale o Cumulus Linux:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-
mlx-amd64.bin
```

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-4.4.3-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-
4.4.3-mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

13. Após a conclusão da instalação, inicie sessão no interrutor.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

14. Verifique a versão Cumulus Linux: `net show version`

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3”
```

Cumulus Linux 5.x

1. Baixe o arquivo de instalação Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo para: `onie-installer`.
2. Conete o host à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interrutor.

   O switch faz o download do instalador de imagem ONIE e inicializa. Após a conclusão da instalação, o prompt de login do Cumulus Linux aparece na janela do terminal.

Cada vez que o Cumulus Linux é instalado, toda a estrutura do sistema de arquivos é apagada e reconstruída.

4. Reinicie o switch SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
.
.
GNU GRUB version 2.06-3
+-------------------------------------------------------------------------
------+
| Cumulus-Linux GNU/Linux
|
| Advanced options for Cumulus-Linux GNU/Linux
|
| ONIE
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
+-------------------------------------------------------------------------
------+
```

5. Pressione a tecla ESC na tela GNU GRUB para interromper o processo de inicialização normal, selecione ONIE e pressione Enter.

```
.
.
Loading ONIE ...

GNU GRUB version 2.02
+-------------------------------------------------------------------------
------+
| ONIE: Install OS
|
| ONIE: Rescue
|
| ONIE: Uninstall OS
|
| ONIE: Update ONIE
|
| ONIE: Embed ONIE
|
|
|
|
|
|
|
|
|
|
|
+-------------------------------------------------------------------------
------+
```

Selecione ONIE: **Instalar os.**

6. O processo de descoberta do instalador ONIE é executado procurando a instalação automática. Pressione **Enter** para interromper temporariamente o processo.
7. Quando o processo de descoberta for interrompido:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process
427:
No such process done.
```

8. Configure o endereço IP, a máscara de sub-rede e o gateway padrão:

```
ifconfig eth0
```

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff
ONIE:/ #
ONIE:/ # ifconfig eth0 10.228.140.27 netmask 255.255.248.0
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet HWaddr B8:CE:F6:5E:05:E6
       inet addr:10.228.140.27 Bcast:10.228.143.255
Mask:255.255.248.0
       inet6 addr: fd20:8b1e:b255:822b:bace:f6ff:fe5e:5e6/64
Scope:Global
       inet6 addr: fe80::bace:f6ff:fe5e:5e6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:18813 errors:0 dropped:1418 overruns:0 frame:0
       TX packets:491 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1339596 (1.2 MiB) TX bytes:49379 (48.2 KiB)
       Memory:dfc00000-dfc1ffff
ONIE:/ # route add default gw 10.228.136.1
ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.228.136.1    0.0.0.0         UG    0      0
0   eth0
10.228.136.1    *               255.255.248.0   U     0      0
0   eth0
```

9. Instale o Cumulus Linux 5,4:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-5.4-mlx-
amd64.bin
```

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-5.4-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-5.4-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

10. Após a conclusão da instalação, inicie sessão no interrutor.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

11. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 13:37:36     system uptime
timezone            Etc/UTC              system time zone
```

12. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Adicione grupos de usuários adicionais para que o usuário admin acesse `nv` comandos:

```
cumulus@cumulus:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

O que se segue?

"Instale o script RCF (Reference Configuration File)".

Atualize versões do Cumulus Linux

Conclua o procedimento a seguir para atualizar sua versão do Cumulus Linux conforme necessário.

Antes de começar

Certifique-se de que tem o seguinte:

- Conhecimento do Linux de nível intermediário.
- Familiaridade com edição de texto básica, permissões de arquivo UNIX e monitoramento de processos. Uma variedade de editores de texto são pré-instalados, `vi` incluindo e `nano`.
- Acesso a um shell Linux ou UNIX. Se você estiver executando o Windows, use um ambiente Linux como sua ferramenta de linha de comando para interagir com o Cumulus Linux.
- O requisito de taxa de transmissão é definido como 115200 no switch de console serial para acesso ao console de switch NVIDIA SN2100, como segue:
  - 115200 baud
  - 8 bits de dados
  - 1 bit de paragem
  - paridade: nenhuma
  - controle de fluxo: nenhum

Sobre esta tarefa

Tenha em atenção o seguinte:

Cada vez que o Cumulus Linux é atualizado, toda a estrutura do sistema de arquivos é apagada e reconstruída. Sua configuração existente será apagada. Você deve salvar e gravar sua configuração de switch antes de atualizar o Cumulus Linux.

A senha padrão para a conta de usuário do Cumulus é **Cumulus**. A primeira vez que você fizer login no Cumulus Linux, você deve alterar essa senha padrão. Você deve atualizar todos os scripts de automação antes de instalar uma nova imagem. O Cumulus Linux fornece opções de linha de comando para alterar a senha padrão automaticamente durante o processo de instalação.

```
https://docs.nvidia.com/networking-ethernet-software/cumulus-linux-
510/Installation-Management/Installing-a-New-Cumulus-Linux-
Image/["Instalando uma nova imagem do Cumulus Linux"^]Consulte para obter
mais informações.
```

Exemplo 3. Passos

Cumulus Linux 4.4.x para Cumulus Linux 5.4.0

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Verifique a versão atual do Cumulus Linux e as portas conetadas:

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox

cumulus@cumulus:mgmt:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  ----------------------
--------------------
.
.
UP     swp1    100G  9216   Trunk/L2    node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2    node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge(UP))
.
.
```

7. Faça o download da imagem Cumulus Linux 5.4.0:

```
cumulus@cumulus:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
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.
```

8. Reinicie o switch:

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

9. Alterar a palavra-passe:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
           operational    applied
---------- -------------- ----------
hostname   cumulus        cumulus
build      Cumulus Linux 5.4.0
uptime     14:07:08
timezone   Etc/UTC
```

11. Altere o nome do host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Termine sessão e inicie sessão novamente no interrutor para ver o nome do interrutor atualizado no aviso:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Defina o endereço IP:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

15. Adicione grupos de usuários adicionais para que o usuário admin acesse `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

Cumulus Linux 5.x para Cumulus Linux 5.4.0

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Verifique a versão atual do Cumulus Linux e as portas conetadas:

```
cumulus@sw1:mgmt:~$ nv show system
                    operational          applied
------------------- -------------------- -----------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0
uptime              6 days, 8:37:36
timezone            Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------- ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01                e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                      swp15
swp
+ swp16      9216 100G    up sw2                      swp16
swp
```

7. Faça o download da imagem Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
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.
```

8. Reinicie o switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Alterar a palavra-passe:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational    applied
-------------- ----------------
hostname       cumulus cumulus
build          Cumulus Linux 5.4.0
uptime         14:07:08
timezone       Etc/UTC
```

11. Altere o nome do host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Termine sessão e inicie sessão novamente no interrutor para ver o nome do interrutor atualizado no aviso:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Defina o endereço IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

15. Adicione grupos de usuários adicionais para que o usuário admin acesse `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

Cumulus Linux 5.4.0 para Cumulus Linux 5.11.0

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Verifique a versão atual do Cumulus Linux e as portas conetadas:

```
cumulus@sw1:mgmt:~$ nv show system
                    operational          applied
------------------- -------------------- -----------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0
uptime              6 days, 8:37:36
timezone            Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------- ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01                e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                      swp15
swp
+ swp16      9216 100G    up sw2                      swp16
swp
```

7. Faça o download da imagem Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
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.
```

8. Reinicie o switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Alterar a palavra-passe:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational    applied
-------------- ----------------
hostname       cumulus cumulus
build          Cumulus Linux 5.11.0
uptime         14:07:08
timezone       Etc/UTC
```

11. Altere o nome do host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Efetue logout e login no switch novamente para ver o nome do switch atualizado no prompt:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Defina o endereço IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

O que se segue?

"Instale ou atualize o script RCF".

Instale ou atualize o script RCF (Reference Configuration File)

Siga este procedimento para instalar ou atualizar o script RCF.

Antes de começar

Antes de instalar ou atualizar o script RCF, certifique-se de que o seguinte está disponível no switch:

- Cumulus Linux está instalado. Consulte "Hardware Universe" para obter as versões suportadas.
- Endereço IP, máscara de sub-rede e gateway padrão definido via DHCP ou configurado manualmente.

Você deve especificar um usuário no RCF (além do usuário admin) para ser usado especificamente para a coleção de logs.

Configurações do cliente

As seguintes categorias de configuração de referência estão disponíveis:

Cluster	Em portas configuradas para breakout 4x10GbE, uma porta é configurada para breakout 4x25GbE e as outras portas são configuradas para 40/100GbE. Suporta tráfego de cluster/HA compartilhado em portas para nós que usam portas de cluster/HA compartilhadas. Veja a tabela de plataformas no artigo da Base de Conhecimento "Quais plataformas AFF, ASA e FAS usam portas Ethernet de cluster e HA compartilhadas?" . Todas as portas também podem ser usadas como portas de cluster dedicadas.
Armazenamento	Todas as portas configuradas para conexões de armazenamento NVMe de 100 GbE.

Versões de script RCF atuais

Há dois scripts RCF disponíveis para aplicativos de cluster e armazenamento. Baixe RCFs "Transferência do software NVIDIA SN2100" da página. O procedimento para cada um é o mesmo.

- Cluster: **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP**
- Armazenamento: **MSN2100-RCF-v1.*x*-Storage**

Sobre os exemplos

O procedimento de exemplo a seguir mostra como baixar e aplicar o script RCF para switches de cluster.

Exemplo de saída de comando usa o endereço IP de gerenciamento de switch 10.233.204.71, máscara de rede 255.255.254.0 e gateway padrão 10.233.204.1.

Exemplo 4. Passos

Cumulus Linux 4.4.3

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

- Se você estiver atualizando seu RCF, deverá desabilitar a reversão automática para esta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desabilitar a reversão automática para esta etapa porque ela já está desabilitada.

1. Apresentar as interfaces disponíveis no interrutor SN2100:

```
admin@sw1:mgmt:~$ net show interface all

State  Name   Spd  MTU    Mode         LLDP                Summary
-----  -----  ---  -----  -----------  ------------------
--------------
...
...
ADMDN  swp1   N/A  9216   NotConfigured
ADMDN  swp2   N/A  9216   NotConfigured
ADMDN  swp3   N/A  9216   NotConfigured
ADMDN  swp4   N/A  9216   NotConfigured
ADMDN  swp5   N/A  9216   NotConfigured
ADMDN  swp6   N/A  9216   NotConfigured
ADMDN  swp7   N/A  9216   NotConfigured
ADMDN  swp8   N/A  9216   NotConfigured
ADMDN  swp9   N/A  9216   NotConfigured
ADMDN  swp10  N/A  9216   NotConfigured
ADMDN  swp11  N/A  9216   NotConfigured
ADMDN  swp12  N/A  9216   NotConfigured
ADMDN  swp13  N/A  9216   NotConfigured
ADMDN  swp14  N/A  9216   NotConfigured
ADMDN  swp15  N/A  9216   NotConfigured
ADMDN  swp16  N/A  9216   NotConfigured
```

2. Copie o script Python do RCF para o switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP         100% 8607
111.2KB/s         00:00
```

> Enquanto `scp` é usado no exemplo, você pode usar seu método preferido de transferência de arquivos, por exemplo SFTP, HTTPS ou FTP.

3. Aplique o script Python RCF **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

O script RCF completa as etapas listadas no exemplo acima.

> No passo 3 **Atualizando o arquivo MOTD** acima, o comando `cat /etc/motd` é executado. Isso permite verificar o nome do arquivo RCF, a versão RCF, as portas a usar e outras informações importantes no banner RCF.

> Para quaisquer problemas de script Python do RCF que não possam ser corrigidos, entre em Contato "Suporte à NetApp" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
5. Verifique a configuração após a reinicialização:

```
admin@sw1:mgmt:~$ net show interface all

State  Name       Spd   MTU    Mode        LLDP               Summary
-----  ---------- ----  -----  ----------  -----------------  --------
...
...
DN     swp1s0     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s1     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s2     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s3     N/A   9216   Trunk/L2                       Master:
```

```
bridge(UP)
DN     swp2s0    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s1    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s2    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s3    N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp3      100G  9216   Trunk/L2                    Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                    Master:
bridge(UP)
DN     swp5      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp6      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp7      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp8      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp9      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp10     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp11     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp12     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp13     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp14     N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp15     N/A   9216   BondMember                  Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                  Master:
bond_15_16(UP)
...
...

admin@sw1:mgmt:~$ net show roce config
RoCE mode.......... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
  Mode........... ECN
  Min Threshold.. 150 KB
```

```
  Max Threshold.. 1500 KB
PFC:
  Status......... enabled
  Enabled SPs.... 2 5
  Interfaces......... swp10-16,swp1s0-3,swp2s0-3,swp3-9

DSCP                     802.1p  switch-priority
-----------------------  ------  ---------------
0 1 2 3 4 5 6 7               0                0
8 9 10 11 12 13 14 15         1                1
16 17 18 19 20 21 22 23       2                2
24 25 26 27 28 29 30 31       3                3
32 33 34 35 36 37 38 39       4                4
40 41 42 43 44 45 46 47       5                5
48 49 50 51 52 53 54 55       6                6
56 57 58 59 60 61 62 63       7                7

switch-priority  TC  ETS
---------------  --  --------
0 1 3 4 6 7       0  DWRR 28%
2                 2  DWRR 28%
5                 5  DWRR 43%
```

6. Verifique as informações do transcetor na interface:

```
admin@sw1:mgmt:~$ net show interface pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor SN
    Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp3       0x11 (QSFP28)  Amphenol     112-00574
APF20379253516  B0
swp4       0x11 (QSFP28)  AVAGO        332-00440        AF1815GU05Z
    A0
swp15      0x11 (QSFP28)  Amphenol     112-00573
APF21109348001  B0
swp16      0x11 (QSFP28)  Amphenol     112-00573
APF21109347895  B0
```

7. Verifique se os nós têm uma conexão com cada switch:

```
admin@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost              RemotePort
---------  -----  ----------  ----------------------  -----------
swp3       100G   Trunk/L2    sw1                     e3a
swp4       100G   Trunk/L2    sw2                     e3b
swp15      100G   BondMember  sw13                    swp15
swp16      100G   BondMember  sw14                    swp16
```

8. Verifique a integridade das portas de cluster no cluster.
   a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

```
cluster1::*> network port show -role cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch SW2, uma vez que LIFs não são homed em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                    Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                       cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                       cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Verifique se o cluster está em bom estado:

   ```
   cluster show
   ```

10. Repita os passos 1 a 14 no segundo interruptor.
11. Ative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

- Se você estiver atualizando seu RCF, deverá desabilitar a reversão automática para esta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desabilitar a reversão automática para esta etapa porque ela já está desabilitada.

1. Apresentar as interfaces disponíveis no interrutor SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------ ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1           Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp
```

2. Copie o script Python do RCF para o switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s         00:00
```

> Enquanto `scp` é usado no exemplo, você pode usar seu método preferido de transferência de arquivos, por exemplo SFTP, HTTPS ou FTP.

3. Aplique o script Python RCF **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

O script RCF completa as etapas listadas no exemplo acima.

> No passo 3 **Atualizando o arquivo MOTD** acima, o comando `cat /etc/issue.net` é executado. Isso permite verificar o nome do arquivo RCF, a versão RCF, as portas a usar e outras informações importantes no banner RCF.

Por exemplo:

```
admin@sw1:mgmt:~$ cat /etc/issue.net
**********************************************************************
**********
*
* NetApp Reference Configuration File (RCF)
* Switch       : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14  : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16 : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
**********************************************************************
**********
```

Para quaisquer problemas de script Python do RCF que não possam ser corrigidos, entre em Contato "Suporte à NetApp" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
5. Verifique a configuração após a reinicialização:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------- ----- ----- ----- ------------------ ------------
--------- -------------
```

```
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                   operational  applied   description
-----------------  -----------  ---------
----------------------------------------
enable             on                     Turn feature 'on' or
'off'. This feature is disabled by default.
mode               lossless     lossless  Roce Mode
congestion-control
  congestion-mode   ECN,RED                Congestion config mode
  enabled-tc        0,2,5                  Congestion config enabled
Traffic Class
  max-threshold     195.31 KB              Congestion config max-
threshold
  min-threshold     39.06 KB               Congestion config min-
threshold
  probability       100
lldp-app-tlv
  priority          3                      switch-priority of roce
  protocol-id       4791                   L4 port number
  selector          UDP                    L4 protocol
pfc
  pfc-priority      2, 5                   switch-prio on which PFC
is enabled
  rx-enabled        enabled                PFC Rx Enabled status
  tx-enabled        enabled                PFC Tx Enabled status
trust
```

```
  trust-mode        pcp,dscp              Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations
========================================
        pcp  dscp                     switch-prio
    --  ---  -----------------------  -----------
    0   0    0,1,2,3,4,5,6,7          0
    1   1    8,9,10,11,12,13,14,15    1
    2   2    16,17,18,19,20,21,22,23  2
    3   3    24,25,26,27,28,29,30,31  3
    4   4    32,33,34,35,36,37,38,39  4
    5   5    40,41,42,43,44,45,46,47  5
    6   6    48,49,50,51,52,53,54,55  6
    7   7    56,57,58,59,60,61,62,63  7

RoCE SP->TC mapping and ETS configurations
==========================================
        switch-prio  traffic-class  scheduler-weight
    --  -----------  -------------  ----------------
    0   0            0              DWRR-28%
    1   1            0              DWRR-28%
    2   2            2              DWRR-28%
    3   3            0              DWRR-28%
    4   4            0              DWRR-28%
    5   5            5              DWRR-43%
    6   6            0              DWRR-28%
    7   7            0              DWRR-28%

RoCE pool config
================
        name                    mode     size  switch-priorities
traffic-class
    --  ----------------------  -------  ----  -----------------
-------------
    0   lossy-default-ingress   Dynamic  50%   0,1,3,4,6,7        -
    1   roce-reserved-ingress   Dynamic  50%   2,5                -
    2   lossy-default-egress    Dynamic  50%   -                  0
    3   roce-reserved-egress    Dynamic  inf   -                  2,5

Exception List
==============
        description
    --
-------------------------------------------------------------------
---…
```

```
    1   RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
    2   Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
    3   Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
    4   Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
    5   Congestion Config max-threshold Mismatch.Expected max-
threshold:
        1500000.
    6   Scheduler config mismatch for traffic-class mapped to
switch-prio0.
        Expected scheduler-weight: DWRR-50%.
    7   Scheduler config mismatch for traffic-class mapped to
switch-prio1.
        Expected scheduler-weight: DWRR-50%.
    8   Scheduler config mismatch for traffic-class mapped to
switch-prio2.
        Expected scheduler-weight: DWRR-50%.
    9   Scheduler config mismatch for traffic-class mapped to
switch-prio3.
        Expected scheduler-weight: DWRR-50%.
    10  Scheduler config mismatch for traffic-class mapped to
switch-prio4.
        Expected scheduler-weight: DWRR-50%.
    11  Scheduler config mismatch for traffic-class mapped to
switch-prio5.
        Expected scheduler-weight: DWRR-50%.
    12  Scheduler config mismatch for traffic-class mapped to
switch-prio6.
        Expected scheduler-weight: strict-priority.
    13  Scheduler config mismatch for traffic-class mapped to
switch-prio7.
        Expected scheduler-weight: DWRR-50%.
    14  Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
    15  Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
    16  Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
    17  Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
    18  Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
    19  Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
```

```
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

> As exceções listadas não afetam o desempenho e podem ser ignoradas com segurança.

6. Verifique as informações do transcetor na interface:

```
admin@sw1:mgmt:~$ nv show interface --view=pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor
SN       Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp1s0     0x00 None
swp1s1     0x00 None
swp1s2     0x00 None
swp1s3     0x00 None
swp2s0     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s1     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s2     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s3     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp3       0x00 None
swp4       0x00 None
swp5       0x00 None
swp6       0x00 None
.
.
.
swp15      0x11 (QSFP28)  Amphenol     112-00595
APF20279210117  B0
swp16      0x11 (QSFP28)  Amphenol     112-00595
APF20279210166  B0
```

7. Verifique se os nós têm uma conexão com cada switch:

```
admin@sw1:mgmt:~$ nv show interface --view=lldp

LocalPort  Speed  Mode        RemoteHost                RemotePort
---------  -----  ----------  ------------------------  -----------
eth0       100M   Mgmt        mgmt-sw1                  Eth110/1/29
swp2s1     25G    Trunk/L2    node1                     e0a
swp15      100G   BondMember  sw2                       swp15
swp16      100G   BondMember  sw2                       swp16
```

8. Verifique a integridade das portas de cluster no cluster.
   a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

```
cluster1::*> network port show -role cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch SW2, uma vez que LIFs não são homed em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                    Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                       cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                       cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Verifique se o cluster está em bom estado:

   ```
   cluster show
   ```

10. Repita os passos 1 a 14 no segundo interruptor.
11. Ative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

4. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      ```
      network port show -role cluster
      ```

   b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

      ```
      network interface show -role cluster
      ```

   c. Verifique se o cluster exibe informações para ambos os switches do cluster:

      ```
      system cluster-switch show -is-monitoring-enabled-operational true
      ```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

- Se você estiver atualizando seu RCF, deverá desabilitar a reversão automática para esta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desabilitar a reversão automática para esta etapa porque ela já está desabilitada.

1. Apresentar as interfaces disponíveis no interrutor SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------ ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1           Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp
```

2. Copie o script Python do RCF para o switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s         00:00
```

> Embora `scp` é usado no exemplo, você pode usar seu método preferido de transferência de arquivos, por exemplo SFTP, HTTPS ou FTP.

3. Aplique o script Python RCF **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

O script RCF completa as etapas listadas no exemplo acima.

Na etapa 3 **Atualizando o arquivo MOTD** acima, o comando `cat /etc/issue.net é executado. Isso permite verificar o nome do arquivo RCF, a versão RCF, as portas a usar e outras informações importantes no banner RCF.

Por exemplo:

```
admin@sw1:mgmt:~$ cat /etc/issue.net
**********************************************************************
**********
*
* NetApp Reference Configuration File (RCF)
* Switch       : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14  : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16 : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
**********************************************************************
**********
```

Para quaisquer problemas de script Python do RCF que não possam ser corrigidos, entre em Contato "Suporte à NetApp" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
5. Verifique a configuração após a reinicialização:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------- ----- ----- ----- ------------------ ------------
--------- -------------
```

```
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                   operational  applied   description
-----------------  -----------  ---------
----------------------------------------
enable             on                     Turn feature 'on' or
'off'. This feature is disabled by default.
mode               lossless     lossless  Roce Mode
congestion-control
  congestion-mode   ECN,RED                Congestion config mode
  enabled-tc        0,2,5                  Congestion config enabled
Traffic Class
  max-threshold     195.31 KB              Congestion config max-
threshold
  min-threshold     39.06 KB               Congestion config min-
threshold
  probability       100
lldp-app-tlv
  priority          3                      switch-priority of roce
  protocol-id       4791                   L4 port number
  selector          UDP                    L4 protocol
pfc
  pfc-priority      2, 5                   switch-prio on which PFC
is enabled
  rx-enabled        enabled                PFC Rx Enabled status
  tx-enabled        enabled                PFC Tx Enabled status
trust
```

```
  trust-mode        pcp,dscp              Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations
========================================
        pcp  dscp                     switch-prio
    --  ---  -----------------------  -----------
    0   0    0,1,2,3,4,5,6,7          0
    1   1    8,9,10,11,12,13,14,15    1
    2   2    16,17,18,19,20,21,22,23  2
    3   3    24,25,26,27,28,29,30,31  3
    4   4    32,33,34,35,36,37,38,39  4
    5   5    40,41,42,43,44,45,46,47  5
    6   6    48,49,50,51,52,53,54,55  6
    7   7    56,57,58,59,60,61,62,63  7

RoCE SP->TC mapping and ETS configurations
==========================================
        switch-prio  traffic-class  scheduler-weight
    --  -----------  -------------  ----------------
    0   0            0              DWRR-28%
    1   1            0              DWRR-28%
    2   2            2              DWRR-28%
    3   3            0              DWRR-28%
    4   4            0              DWRR-28%
    5   5            5              DWRR-43%
    6   6            0              DWRR-28%
    7   7            0              DWRR-28%

RoCE pool config
================
        name                    mode     size  switch-priorities
traffic-class
    --  ----------------------  -------  ----  -----------------
-------------
    0   lossy-default-ingress   Dynamic  50%   0,1,3,4,6,7        -
    1   roce-reserved-ingress   Dynamic  50%   2,5                -
    2   lossy-default-egress    Dynamic  50%   -                  0
    3   roce-reserved-egress    Dynamic  inf   -                  2,5

Exception List
==============
        description
    --
-------------------------------------------------------------------
---…
```

```
    1   RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
    2   Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
    3   Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
    4   Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
    5   Congestion Config max-threshold Mismatch.Expected max-
threshold:
        1500000.
    6   Scheduler config mismatch for traffic-class mapped to
switch-prio0.
        Expected scheduler-weight: DWRR-50%.
    7   Scheduler config mismatch for traffic-class mapped to
switch-prio1.
        Expected scheduler-weight: DWRR-50%.
    8   Scheduler config mismatch for traffic-class mapped to
switch-prio2.
        Expected scheduler-weight: DWRR-50%.
    9   Scheduler config mismatch for traffic-class mapped to
switch-prio3.
        Expected scheduler-weight: DWRR-50%.
    10  Scheduler config mismatch for traffic-class mapped to
switch-prio4.
        Expected scheduler-weight: DWRR-50%.
    11  Scheduler config mismatch for traffic-class mapped to
switch-prio5.
        Expected scheduler-weight: DWRR-50%.
    12  Scheduler config mismatch for traffic-class mapped to
switch-prio6.
        Expected scheduler-weight: strict-priority.
    13  Scheduler config mismatch for traffic-class mapped to
switch-prio7.
        Expected scheduler-weight: DWRR-50%.
    14  Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
    15  Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
    16  Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
    17  Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
    18  Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
    19  Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
```

```
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

> As exceções listadas não afetam o desempenho e podem ser ignoradas com segurança.

6. Verifique as informações do transcetor na interface:

```
admin@sw1:mgmt:~$ nv show platform transceiver
Interface  Identifier     Vendor Name  Vendor PN        Vendor
SN       Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp1s0     0x00 None
swp1s1     0x00 None
swp1s2     0x00 None
swp1s3     0x00 None
swp2s0     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s1     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s2     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s3     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp3       0x00 None
swp4       0x00 None
swp5       0x00 None
swp6       0x00 None
.
.
.
swp15      0x11 (QSFP28)  Amphenol     112-00595
APF20279210117  B0
swp16      0x11 (QSFP28)  Amphenol     112-00595
APF20279210166  B0
```

7. Verifique se os nós têm uma conexão com cada switch:

```
admin@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost                RemotePort
---------  -----  ----------  ------------------------  -----------
eth0       100M   Mgmt        mgmt-sw1                  Eth110/1/29
swp2s1     25G    Trunk/L2    node1                     e0a
swp15      100G   BondMember  sw2                       swp15
swp16      100G   BondMember  sw2                       swp16
```

8. Verifique a integridade das portas de cluster no cluster.
   a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

```
cluster1::*> network port show -role cluster

Node: node1

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch SW2, uma vez que LIFs não são homed em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                    Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                       cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                       cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Verifique se o cluster está em bom estado:

   ```
   cluster show
   ```

10. Repita os passos 1 a 14 no segundo interruptor.
11. Ative a reversão automática nos LIFs do cluster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

O que se segue?

"Instale o arquivo CSHM".

Instale o arquivo de configuração do Monitor de integridade do comutador Ethernet

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 conetados.

     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
   ```

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 show` no sistema ONTAP e certifique-se de que os switches de cluster são descobertos com o campo monitorado definido como **True** e o campo de número de série não mostrando **desconhecido**.

```
cluster1::> system switch ethernet 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".

Redefinir o switch do cluster SN2100 para os padrões de fábrica

Para redefinir o switch do cluster SN2100 para os padrões de fábrica:

- Para o Cumulus Linux 5.10 e anteriores, aplique a imagem Cumulus.
- Para Cumulus Linux 5.11 e posterior, você usa o `nv action reset system factory-default` comando.

Sobre esta tarefa

- Você deve estar conetado ao switch usando o console serial.
- Você precisa ter a senha de root para ter acesso sudo aos comandos.

Para obter mais informações sobre a instalação do Cumulus Linux, consulte"Fluxo de trabalho de instalação de software para switches NVIDIA SN2100" .

Exemplo 5. Passos

Cumulus Linux 5.10 e anteriores

1. No console Cumulus, baixe e coloque na fila a instalação do software do switch com o comando `onie-install -a -i` seguido pelo caminho do arquivo para o software do switch, por exemplo:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. O instalador inicia o download. Digite **y** quando solicitado para confirmar a instalação quando a imagem for baixada e verificada.
3. Reinicie o switch para instalar o novo software.

   `sudo reboot`

```
cumulus@sw1:mgmt:~$ sudo reboot
```

> O switch é reinicializado e entra na instalação do software do switch, o que leva algum tempo. Quando a instalação estiver concluída, o switch será reinicializado e permanecerá no estado `log-in` incitar.

Cumulus Linux 5.11 e posterior

1. Para redefinir o switch para os padrões de fábrica e remover todas as configurações, arquivos de sistema e arquivos de log, execute:

   `nv action reset system factory-default`

   Por exemplo:

```
cumulus@switch:~$ nv action reset system factory-default

This operation will reset the system configuration, delete the log
files and reboot the switch.
Type [y] continue.
Type [n] to abort.
Do you want to continue? [y/n] y
```

Veja a NVIDIA "Redefinição de fábrica" documentação para mais detalhes.

Migrar os switches

Migre os switches de cluster CN1610 para os switches de cluster NVIDIA SN2100

É possível migrar os switches de cluster do NetApp CN1610 para um cluster do ONTAP para os switches de cluster do NVIDIA SN2100. Este é um procedimento sem interrupções.

Rever os requisitos

Você deve estar ciente de certas informações de configuração, conexões de portas e requisitos de cabeamento ao substituir os switches de cluster NetApp CN1610 por switches de cluster NVIDIA SN2100. "Visão geral da instalação e configuração dos switches NVIDIA SN2100"Consulte .

Interrutores suportados

Os seguintes switches de cluster são suportados:

- NetApp CN1610
- NVIDIA SN2100

Para obter detalhes sobre as portas suportadas e suas configurações, consulte o "Hardware Universe".

Antes de começar

Verifique se você atende aos seguintes requisitos para sua configuração:

- O cluster existente está corretamente configurado e funcionando.
- Todas as portas de cluster estão no estado **up** para garantir operações ininterruptas.
- Os switches de cluster NVIDIA SN2100 são configurados e operando sob a versão correta do Cumulus Linux instalado com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede de cluster existente tem o seguinte:
  - Um cluster NetApp redundante e totalmente funcional usando switches CN1610.
  - Conetividade de gerenciamento e acesso ao console aos switches CN1610 e aos novos switches.
  - Todos os LIFs de cluster no estado up com os LIfs de cluster em suas portas iniciais.
  - Portas ISL ativadas e cabeadas entre os switches CN1610 e entre os novos switches.
- Algumas das portas são configuradas nos switches NVIDIA SN2100 para serem executadas em 40GbE ou 100GbE.
- Você planejou, migrou e documentou a conectividade 40GbE e 100GbE de nós para os switches de cluster NVIDIA SN2100.

Migrar os switches

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de cluster CN1610 existentes são *C1* e *C2*.
- Os novos switches de cluster do NVIDIA SN2100 são *SW1* e *SW2*.
- Os nós são *node1* e *node2*.
- Os LIFs de cluster são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.

- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *E3A* e *e3b*.
- As portas breakout tomam o formato: swp[port]s[breakout port 0-3]. Por exemplo, quatro portas breakout no swp1 são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O interrutor C2 é substituído primeiro pelo interrutor SW2.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - O cabeamento entre os nós e o C2 é desconetado do C2 e reconetado ao SW2.
- O interrutor C1 é substituído pelo interrutor SW1.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - O cabeamento entre os nós e o C1 é desconetado do C1 e reconetado ao SW1.

> Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

3. Desativar a reversão automática nos LIFs do cluster:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

Etapa 2: Configurar portas e cabeamento

1. Determine o status administrativo ou operacional de cada interface de cluster.

   Cada porta deve ser exibida durante `Link` e `healthy` para `Health Status`.

   a. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

b. Exibir informações sobre os LIFs e seus nós iniciais designados:

```
network interface show -vserver Cluster
```

Cada LIF deve ser exibido `up/up` para `Status Admin/Oper` e `true` para `Is Home`.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. As portas de cluster em cada nó são conetadas aos switches de cluster existentes da seguinte maneira (da perspetiva dos nós) usando o comando:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e3a    c1 (6a:ad:4f:98:3b:3f)    0/1               -
            e3b    c2 (6a:ad:4f:98:4c:a4)    0/1               -
node2      /cdp
            e3a    c1 (6a:ad:4f:98:3b:3f)    0/2               -
            e3b    c2 (6a:ad:4f:98:4c:a4)    0/2               -
```

3. As portas e os switches do cluster são conetados da seguinte maneira (da perspetiva dos switches) usando o comando:

   `show cdp neighbors`

Mostrar exemplo

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124     H          AFF-A400
e3a
node2                 0/2           124     H          AFF-A400
e3a
c2                    0/13          179     S I s      CN1610
0/13
c2                    0/14          175     S I s      CN1610
0/14
c2                    0/15          179     S I s      CN1610
0/15
c2                    0/16          175     S I s      CN1610
0/16

c2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124    H           AFF-A400
e3b
node2                 0/2           124    H           AFF-A400
e3b
c1                    0/13          175    S I s       CN1610
0/13
c1                    0/14          175    S I s       CN1610
0/14
c1                    0/15          175    S I s       CN1610
0/15
c1                    0/16          175    S I s       CN1610
0/16
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. no switch C2, encerre as portas conetadas às portas do cluster dos nós para fazer failover dos LIFs do cluster.

```
(c2)# configure
(c2)(Config)# interface 0/1-0/12
(c2)(Interface 0/1-0/12)# shutdown
(c2)(Interface 0/1-0/12)# exit
(c2)(Config)# exit
(c2)#
```

2. Mova as portas do cluster de nós do switch antigo C2 para o novo switch SW2, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
3. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

4. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   0/1               -
            e3b    sw2 (b8:ce:f6:19:1a:7e)   swp3              -
node2      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   0/2               -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4              -
```

5. No switch SW2, verifique se todas as portas do cluster de nós estão ativas:

   `net show interface`

Mostrar exemplo

```
cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

6. No switch C1, encerre as portas conetadas às portas do cluster dos nós para fazer failover das LIFs do cluster.

```
(c1)# configure
(c1)(Config)# interface 0/1-0/12
(c1)(Interface 0/1-0/12)# shutdown
(c1)(Interface 0/1-0/12)# exit
(c1)(Config)# exit
(c1)#
```

7. Mova as portas do cluster de nós do switch antigo C1 para o novo switch SW1, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
8. Verifique a configuração final do cluster:

   `network port show -ipspace Cluster`

   Cada porta deve ser exibida `up` para `Link` e `healthy` para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

9. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3           -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4           -
```

10. Nos switches SW1 e SW2, verifique se todas as portas do cluster de nós estão ativas:

    `net show interface`

Mostrar exemplo

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw2 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw2 (swp16)
Master: cluster_isl(UP)


cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

11. Verifique se ambos os nós têm uma conexão com cada switch:

    `net show lldp`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3a
swp4       100G   Trunk/L2    node2               e3a
swp15      100G   BondMember  sw2                 swp15
swp16      100G   BondMember  sw2                 swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3b
swp4       100G   Trunk/L2    node2               e3b
swp15      100G   BondMember  sw1                 swp15
swp16      100G   BondMember  sw1                 swp16
```

Etapa 3: Verifique a configuração

1. Ativar a reversão automática nos LIFs do cluster:

   ```
   cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
   true
   ```

2. Verifique se todas as LIFs de rede do cluster estão de volta em suas portas domésticas:

   ```
   network interface show
   ```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
```

3. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

4. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migre de um switch de cluster Cisco para um switch de cluster NVIDIA SN2100

É possível migrar os switches de cluster do Cisco para um cluster do ONTAP para os switches de cluster do NVIDIA SN2100. Este é um procedimento sem interrupções.

Rever os requisitos

Você deve estar ciente de certas informações de configuração, conexões de portas e requisitos de cabeamento ao substituir alguns switches de cluster Cisco mais antigos por switches de cluster NVIDIA SN2100. "Visão geral da instalação e configuração dos switches NVIDIA SN2100"Consulte .

Interrutores suportados

Os seguintes switches de cluster Cisco são suportados:

- Nexus 9336C-FX2
- Nexus 92300YC

- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Para obter detalhes sobre as portas suportadas e suas configurações, consulte o "Hardware Universe" .

O que você vai precisar

Certifique-se de que:

- O cluster existente está corretamente configurado e funcionando.
- Todas as portas de cluster estão no estado **up** para garantir operações ininterruptas.
- Os switches de cluster NVIDIA SN2100 são configurados e operando sob a versão adequada do Cumulus Linux instalado com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede de cluster existente tem o seguinte:
  - Um cluster NetApp redundante e totalmente funcional usando ambos os switches Cisco mais antigos.
  - Conetividade de gerenciamento e acesso ao console aos switches Cisco mais antigos e aos novos switches.
  - Todas as LIFs de cluster no estado up com os LIfs de cluster estão em suas portas iniciais.
  - Portas ISL ativadas e cabeadas entre os switches Cisco mais antigos e entre os novos switches.
- Algumas das portas são configuradas nos switches NVIDIA SN2100 para serem executadas a 40 GbE ou 100 GbE.
- Você planejou, migrou e documentou a conectividade de 40 GbE e 100 GbE de nós para os switches de cluster NVIDIA SN2100.

> Se você estiver alterando a velocidade da porta das portas de cluster e0a e e1a em sistemas AFF A800 ou AFF C800, você pode observar pacotes mal formados sendo recebidos após a conversão de velocidade. Consulte "Erro 1570339" e o artigo da base de dados de Conhecimento "Erros de CRC em portas T6 após a conversão de 40GbE para 100GbE" para obter orientação.

Migrar os switches

Sobre os exemplos

Neste procedimento, os switches de cluster Cisco Nexus 3232C são usados, por exemplo, comandos e saídas.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de cluster Cisco Nexus 3232C existentes são *C1* e *C2*.
- Os novos switches de cluster do NVIDIA SN2100 são *SW1* e *SW2*.
- Os nós são *node1* e *node2*.
- Os LIFs de cluster são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *E3A* e *e3b*.

- As portas breakout tomam o formato: swp[port]s[breakout port 0-3]. Por exemplo, quatro portas breakout no swp1 são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O interrutor C2 é substituído primeiro pelo interrutor SW2.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - O cabeamento entre os nós e o C2 é desconetado do C2 e reconetado ao SW2.
- O interrutor C1 é substituído pelo interrutor SW1.
  - Encerre as portas para os nós de cluster. Todas as portas devem ser fechadas simultaneamente para evitar a instabilidade do cluster.
  - O cabeamento entre os nós e o C1 é desconetado do C1 e reconetado ao SW1.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

3. Desativar a reversão automática nos LIFs do cluster:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

Etapa 2: Configurar portas e cabeamento

1. Determine o status administrativo ou operacional de cada interface de cluster.

   Cada porta deve ser exibida para `Link` e saudável para `Health Status`.

   a. Exibir os atributos da porta de rede:

      ```
      network port show -ipspace Cluster
      ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

b. Exibir informações sobre as interfaces lógicas e seus nós iniciais designados:

`network interface show -vserver Cluster`

Cada LIF deve ser exibido `up/up` para `Status Admin/Oper` e verdadeiro para `Is Home`.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. As portas de cluster em cada nó são conetadas aos switches de cluster existentes da seguinte maneira (da perspetiva dos nós):

   `network device-discovery show -protocol lldp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/1            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/1            -
node2      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/2            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/2            -
```

3. As portas e os switches do cluster são conetados da seguinte maneira (da perspetiva dos switches):

   `show cdp neighbors`

Mostrar exemplo

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1         124   H           AFF-A400
e3a
node2                 Eth1/2         124   H           AFF-A400
e3a
c2                    Eth1/31        179   S I s       N3K-C3232C
Eth1/31
c2                    Eth1/32        175   S I s       N3K-C3232C
Eth1/32

c2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
c1                    Eth1/31       175    S I s       N3K-C3232C
Eth1/31
c1                    Eth1/32       175    S I s       N3K-C3232C
Eth1/32
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. no switch C2, encerre as portas conetadas às portas do cluster dos nós para fazer failover dos LIFs do cluster.

```
(c2)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2)(Config)# interface
(c2)(config-if-range)# shutdown <interface_list>
(c2)(config-if-range)# exit
(c2)(Config)# exit
(c2)#
```

2. Mova as portas do cluster de nós do switch antigo C2 para o novo switch SW2, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
3. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

4. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/1            -
            e3b    sw2 (b8:ce:f6:19:1a:7e)   swp3              -
node2      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/2            -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4              -
```

5. No switch SW2, verifique se todas as portas do cluster de nós estão ativas:

   `net show interface`

Mostrar exemplo

```
cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

6. No switch C1, encerre as portas conetadas às portas do cluster dos nós para fazer failover das LIFs do cluster.

```
(c1)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1)(Config)# interface
(c1)(config-if-range)# shutdown <interface_list>
(c1)(config-if-range)# exit
(c1)(Config)# exit
(c1)#
```

7. Mova as portas do cluster de nós do switch antigo C1 para o novo switch SW1, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
8. Verifique a configuração final do cluster:

   `network port show -ipspace Cluster`

   Cada porta deve ser exibida `up` para `Link` e saudável para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace    Broadcast Domain Link MTU   Admin/Oper   Status
Status
--------- ---------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster    Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster    Cluster          up   9000  auto/100000
healthy  false
```

9. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3           -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4           -
```

10. Nos switches SW1 e SW2, verifique se todas as portas do cluster de nós estão ativas:

    `net show interface`

Mostrar exemplo

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw2 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw2 (swp16)
Master: cluster_isl(UP)


cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

11. Verifique se ambos os nós têm uma conexão com cada switch:

    `net show lldp`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3a
swp4       100G   Trunk/L2    node2               e3a
swp15      100G   BondMember  sw2                 swp15
swp16      100G   BondMember  sw2                 swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3b
swp4       100G   Trunk/L2    node2               e3b
swp15      100G   BondMember  sw1                 swp15
swp16      100G   BondMember  sw1                 swp16
```

Etapa 3: Verifique a configuração

1. Ativar a reversão automática nos LIFs do cluster:

   ```
   cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
   true
   ```

2. Verifique se todas as LIFs de rede do cluster estão de volta em suas portas domésticas:

   ```
   network interface show
   ```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
```

3. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

4. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migre para um cluster comutado de dois nós com os switches de cluster NVIDIA SN2100

Se você tiver um ambiente de cluster sem switch de dois nós existente, poderá migrar para um ambiente de cluster comutado de dois nós usando os switches NVIDIA SN2100 para permitir que você escale além de dois nós no cluster.

O procedimento usado depende se você tem duas portas de rede de cluster dedicadas em cada controlador ou uma única porta de cluster em cada controlador. O processo documentado funciona para todos os nós que usam portas óticas ou Twinax, mas não é suportado neste switch se os nós estiverem usando portas 10GBASEBASE-T RJ45 integradas para as portas de cluster-rede.

Rever os requisitos

Configuração sem switch de dois nós

Certifique-se de que:

- A configuração sem switch de dois nós está configurada e funcionando corretamente.
- Os nós estão executando o ONTAP 9.10.1P3 e posterior.
- Todas as portas de cluster estão no estado **up**.
- Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e em suas portas domésticas.

Configuração do switch de cluster do NVIDIA SN2100

Certifique-se de que:

- Ambos os switches têm conetividade de rede de gerenciamento.
- Existe acesso à consola aos interrutores do cluster.
- As conexões de switch de nó para nó NVIDIA SN2100 e switch para switch usam cabos Twinax ou fibra.

> "Analise as considerações sobre cabeamento e configuração"Consulte para ver as ressalvas e mais detalhes. O "Hardware Universe - interrutores" também contém mais informações sobre cabeamento.

- Os cabos ISL (Inter-Switch Link) são conetados às portas swp15 e swp16 em ambos os switches NVIDIA SN2100.
- A personalização inicial de ambos os switches SN2100 está concluída, de modo que:
  - Os switches SN2100 estão executando a versão mais recente do Cumulus Linux
  - Os arquivos de configuração de referência (RCFs) são aplicados aos switches
  - Qualquer personalização de site, como SMTP, SNMP e SSH, é configurada nos novos switches.

    O "Hardware Universe" contém as informações mais recentes sobre as portas de cluster reais para as suas plataformas.

Migrar os switches

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches SN2100 são *SW1* e *SW2*.
- Os nomes dos SVMs do cluster são *node1* e *node2*.
- Os nomes dos LIFs são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *E3A* e *e3b*.
- As portas breakout tomam o formato: swp[port]s[breakout port 0-3]. Por exemplo, quatro portas breakout no swp1 são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar: `set -privilege advanced`

   (`*>`É apresentado o aviso avançado).

Etapa 2: Configurar portas e cabeamento

Cumulus Linux 4,4.x

1. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster SW1 e SW2.

   Não deve desativar as portas ISL.

   Os comandos a seguir desativam as portas voltadas para o nó nos switches SW1 e SW2:

   ```
   cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit

   cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw2:~$ net pending
   cumulus@sw2:~$ net commit
   ```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches SN2100 SW1 e SW2 estão acima nas portas swp15 e swp16:

   ```
   net show interface
   ```

   Os comandos a seguir mostram que as portas ISL estão ativadas nos switches SW1 e SW2:

```
cumulus@sw1:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
-----------------------
...
...
UP     swp15      100G  9216   BondMember  sw2 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw2 (swp16)  Master:
cluster_isl(UP)

cumulus@sw2:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
-----------------------
...
...
UP     swp15      100G  9216   BondMember  sw1 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw1 (swp16)  Master:
cluster_isl(UP)
```

Cumulus Linux 5.x

1. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster SW1 e SW2.

   Não deve desativar as portas ISL.

   Os comandos a seguir desativam as portas voltadas para o nó nos switches SW1 e SW2:

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
down
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save

cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
down
cumulus@sw2:~$ nv config apply
cumulus@sw2:~$ nv config save
```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches SN2100 SW1 e SW2 estão acima nas portas swp15 e swp16:

```
nv show interface
```

Os exemplos a seguir mostram que as portas ISL estão ativadas nos switches SW1 e SW2:

```
cumulus@sw1:~$ nv show interface

Interface     MTU    Speed  State  Remote Host  Remote Port
Type    Summary
------------- ------ -----  ------ ------------
----------------------------------- ------- -------
...
...
+ swp14       9216          down
swp
+ swp15       9216   100G   up     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-rcf2    Intra-Cluster Switch
ISL Port swp16  swp


cumulus@sw2:~$ nv show interface

Interface     MTU    Speed  State  Remote Host  Remote Port
Type    Summary
------------- ------ -----  ------ ------------
----------------------------------- ------- -------
...
...
+ swp14       9216          down
swp
+ swp15       9216   100G   up     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-rcf2    Intra-Cluster Switch
ISL Port swp16  swp
```

1. Verifique se todas as portas de cluster estão ativas:

```
network port show
```

Cada porta deve ser exibida `up` para `Link` e saudável para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show

Node: node1


Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false

Node: node2


Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false
```

2. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show`

   Cada LIF de cluster deve exibir true para `Is Home` e ter um `Status Admin/Oper` de `up/up`.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
```

3. Desativar a reversão automática nos LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert false`

   Mostrar exemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   false
          node1_clus2   false
          node2_clus1   false
          node2_clus2   false
```

4. Desconete o cabo da porta de cluster E3A no node1 e conete o E3A à porta 3 no switch de cluster SW1, usando o cabeamento apropriado suportado pelos switches SN2100.

   O "Hardware Universe - interrutores" contém mais informações sobre cabeamento.

5. Desconete o cabo da porta de cluster E3A no node2 e conete o E3A à porta 4 no switch de cluster SW1,

usando o cabeamento apropriado suportado pelos switches SN2100.

Cumulus Linux 4,4.x

1. no switch SW1, habilite todas as portas voltadas para o nó.

   Os comandos a seguir habilitam todas as portas voltadas para o nó no switch SW1.

   ```
   cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

2. no switch SW1, verifique se todas as portas estão ativas:

   ```
   net show interface all
   ```

```
cumulus@sw1:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP             Summary
-----  --------- ----  -----  ---------- ---------------- --------
...
DN     swp1s0    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s1    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s2    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s3    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s0    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s1    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s2    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s3    25G   9216   Trunk/L2                    Master:
br_default(UP)
UP     swp3      100G  9216   Trunk/L2    node1 (e3a)     Master:
br_default(UP)
UP     swp4      100G  9216   Trunk/L2    node2 (e3a)     Master:
br_default(UP)
...
...
UP     swp15     100G  9216   BondMember  swp15           Master:
cluster_isl(UP)
UP     swp16     100G  9216   BondMember  swp16           Master:
cluster_isl(UP)
...
```

Cumulus Linux 5.x

1. no switch SW1, habilite todas as portas voltadas para o nó.

   Os comandos a seguir habilitam todas as portas voltadas para o nó no switch SW1.

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
up
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

2. no switch SW1, verifique se todas as portas estão ativas:

```
nv show interface
```

```
cumulus@sw1:~$ nv show interface

Interface    State  Speed  MTU    Type      Remote Host
Remote Port  Summary
-----------  -----  -----  -----  --------
--------------------------  -----------  ----------
...
...
swp1s0       up     10G    9216   swp       odq-a300-1a
e0a
swp1s1       up     10G    9216   swp       odq-a300-1b
e0a
swp1s2       down   10G    9216   swp
swp1s3       down   10G    9216   swp
swp2s0       down   25G    9216   swp
swp2s1       down   25G    9216   swp
swp2s2       down   25G    9216   swp
swp2s3       down   25G    9216   swp
swp3         down          9216   swp
swp4         down          9216   swp
...
...
swp14        down          9216   swp
swp15        up     100G   9216   swp       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-int-rcf10
swp16
```

1. Verifique se todas as portas de cluster estão ativas:

```
network port show -ipspace Cluster
```

Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão em node1 e node2:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false
```

2. Exibir informações sobre o status dos nós no cluster:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
```

3. Desconete o cabo da porta de cluster e3b no node1 e conete o e3b à porta 3 no switch de cluster SW2, usando o cabeamento apropriado suportado pelos switches SN2100.
4. Desconete o cabo da porta de cluster e3b no node2 e conete o e3b à porta 4 no switch de cluster SW2, usando o cabeamento apropriado suportado pelos switches SN2100.

Cumulus Linux 4,4.x

1. no switch SW2, habilite todas as portas voltadas para o nó.

   Os comandos a seguir habilitam as portas voltadas para o nó no switch SW2:

   ```
   cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw2:~$ net pending
   cumulus@sw2:~$ net commit
   ```

2. no switch SW2, verifique se todas as portas estão ativas:

   ```
   net show interface all
   ```

```
cumulus@sw2:~$ net show interface all

State  Name      Spd   MTU    Mode        LLDP             Summary
-----  --------- ----  -----  ---------- ---------------- --------
...
DN     swp1s0    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s1    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s2    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s3    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s0    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s1    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s2    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s3    25G   9216   Trunk/L2                    Master:
br_default(UP)
UP     swp3      100G  9216   Trunk/L2    node1 (e3b)     Master:
br_default(UP)
UP     swp4      100G  9216   Trunk/L2    node2 (e3b)     Master:
br_default(UP)
...
...
UP     swp15     100G  9216   BondMember  swp15           Master:
cluster_isl(UP)
UP     swp16     100G  9216   BondMember  swp16           Master:
cluster_isl(UP)
...
```

3. em ambos os switches SW1 e SW2, verifique se ambos os nós têm uma conexão para cada switch:

   `net show lldp`

   O exemplo a seguir mostra os resultados apropriados para ambos os switches SW1 e SW2:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3b
swp4       100G   Trunk/L2    node2              e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

Cumulus Linux 5.x

1. no switch SW2, habilite todas as portas voltadas para o nó.

   Os comandos a seguir habilitam as portas voltadas para o nó no switch SW2:

   ```
   cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
   up
   cumulus@sw2:~$ nv config apply
   cumulus@sw2:~$ nv config save
   ```

2. no switch SW2, verifique se todas as portas estão ativas:

   ```
   nv show interface
   ```

```
cumulus@sw2:~$ nv show interface

Interface    State  Speed  MTU    Type      Remote Host
Remote Port  Summary
-----------  -----  -----  -----  --------
--------------------------  -----------  ----------
...
...
swp1s0       up     10G    9216   swp       odq-a300-1a
e0a
swp1s1       up     10G    9216   swp       odq-a300-1b
e0a
swp1s2       down   10G    9216   swp
swp1s3       down   10G    9216   swp
swp2s0       down   25G    9216   swp
swp2s1       down   25G    9216   swp
swp2s2       down   25G    9216   swp
swp2s3       down   25G    9216   swp
swp3         down          9216   swp
swp4         down          9216   swp
...
...
swp14        down          9216   swp
swp15        up     100G   9216   swp       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-int-rcf10
swp16
```

3. em ambos os switches SW1 e SW2, verifique se ambos os nós têm uma conexão para cada switch:

   `nv show interface --view=lldp`

   Os exemplos a seguir mostram os resultados apropriados para ambos os switches SW1 e SW2:

```
cumulus@sw1:~$ nv show interface --view=lldp

Interface    Speed  Type      Remote Host
Remote Port
-----------  -----  --------  ---------------------------------
-----------
...
...
swp1s0       10G    swp       odq-a300-1a
e0a
```

```
swp1s1       10G    swp       odq-a300-1b
e0a
swp1s2       10G    swp
swp1s3       10G    swp
swp2s0       25G    swp
swp2s1       25G    swp
swp2s2       25G    swp
swp2s3       25G    swp
swp3                swp
swp4                swp
...
...
swp14               swp
swp15        100G   swp       ossg-int-rcf10
swp15
swp16        100G   swp       ossg-int-rcf10
swp16

cumulus@sw2:~$ nv show interface --view=lldp

Interface    Speed  Type      Remote Host
Remote Port
-----------  -----  --------  ---------------------------------
-----------
...
...
swp1s0       10G    swp       odq-a300-1a
e0a
swp1s1       10G    swp       odq-a300-1b
e0a
swp1s2       10G    swp
swp1s3       10G    swp
swp2s0       25G    swp
swp2s1       25G    swp
swp2s2       25G    swp
swp2s3       25G    swp
swp3                swp
swp4                swp
...
...
swp14               swp
swp15        100G   swp       ossg-int-rcf10
swp15
swp16        100G   swp       ossg-int-rcf10
swp16
```

1. exiba informações sobre os dispositivos de rede descobertos em seu cluster:

   ```
   network device-discovery show -protocol lldp
   ```

   Mostrar exemplo

   ```
   cluster1::*> network device-discovery show -protocol lldp
   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
   ----------- ------ ------------------------- ------------
   ----------------
   node1      /lldp
               e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3          -
               e3b    sw2 (b8:ce:f6:19:1b:96)   swp3          -
   node2      /lldp
               e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4          -
               e3b    sw2 (b8:ce:f6:19:1b:96)   swp4          -
   ```

2. Verifique se todas as portas do cluster estão ativas:

   ```
   network port show -ipspace Cluster
   ```

Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão em node1 e node2:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Etapa 3: Verifique a configuração

1. Ativar a reversão automática em todas as LIFs do cluster:

   ```
   net interface modify -vserver Cluster -lif * -auto-revert true
   ```

Mostrar exemplo

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto
-revert true

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true
```

2. Verifique se todas as interfaces são exibidas `true` para `Is Home`:

   `net interface show -vserver Cluster`

   Isso pode levar um minuto para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> net interface show -vserver Cluster

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e3a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e3b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e3a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e3b
true
```

3. Verifique se as definições estão desativadas:

   `network options switchless-cluster show`

   Mostrar exemplo

   A saída falsa no exemplo a seguir mostra que as configurações estão desativadas:

   ```
   cluster1::*> network options switchless-cluster show
   Enable Switchless Cluster: false
   ```

4. Verifique o status dos membros do nó no cluster:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

   ```
   cluster1::*> cluster show

   Node                 Health  Eligibility   Epsilon
   -------------------- ------- ------------  --------
   node1                true    true          false
   node2                true    true          false
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os interruptores

Substitua um interrutor do cluster do NVIDIA SN2100

Siga este procedimento para substituir um switch NVIDIA SN2100 defeituoso em uma rede de cluster. Este é um procedimento sem interrupções (NDU).

Rever os requisitos

Infraestrutura de cluster e rede existentes

Certifique-se de que:

- O cluster existente é verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
- Todas as portas do cluster estão ativas.
- Todas as interfaces lógicas de cluster (LIFs) estão ativas e em suas portas domésticas.
- O comando ONTAP `cluster ping-cluster -node node1` indica que a conetividade básica e maior que a comunicação PMTU são bem-sucedidas em todos os caminhos.

Interrutor de substituição NVIDIA SN2100

Certifique-se de que:

- A conetividade de rede de gerenciamento no switch de substituição está funcional.
- O acesso do console ao interrutor de substituição está no lugar.
- As conexões do nó são as portas swp1 a swp14.
- Todas as portas ISL (Inter-Switch Link) estão desativadas nas portas swp15 e swp16.
- O arquivo de configuração de referência desejado (RCF) e o comutador de imagem do sistema operacional Cumulus são carregados no switch.
- A personalização inicial do switch está concluída.

Certifique-se também de que todas as personalizações anteriores do site, como STP, SNMP e SSH, sejam copiadas para o novo switch.

> Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desativar a criação de casos durante a manutenção. Consulte este artigo da base de dados de Conhecimento "SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para obter mais detalhes.
- Ativar o registo de sessão para quaisquer sessões CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" neste artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Substitua o interrutor

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches NVIDIA SN2100 existentes são *SW1* e *SW2*.
- O nome do novo switch NVIDIA SN2100 é *nsw2*.
- Os nomes dos nós são *node1* e *node2*.
- As portas de cluster em cada nó são chamadas *E3A* e *e3b*.

- Os nomes de LIF do cluster são *node1_clus1* e *node1_clus2* para node1, e *node2_clus1* e *node2_clus2* para node2.
- O prompt para alterações em todos os nós de cluster é `cluster1::*>`
- As portas breakout tomam o formato: swp[port]s[breakout port 0-3]. Por exemplo, quatro portas breakout no swp1 são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre a topologia da rede do cluster

Este procedimento baseia-se na seguinte topologia de rede de cluster:

Mostrar exemplo de topologia

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper   Status
Status
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper   Status
Status
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e3a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e3b
true
```

```
            node2_clus1  up/up    169.254.47.194/16  node2         e3a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e3b
true


cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3          -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4          -
```

E

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw2                e3a
swp4       100G   Trunk/L2    sw2                e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16


cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw1                e3b
swp4       100G   Trunk/L2    sw1                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

Passo 1: Prepare-se para a substituição

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

3. Instale o RCF e a imagem apropriados no interrutor, nsw2, e faça os preparativos necessários para o local.

   Se necessário, verifique, baixe e instale as versões apropriadas do software RCF e Cumulus para o novo switch.

   a. Você pode baixar o software Cumulus aplicável para suas centrais de cluster no site *suporte NVIDIA*. Siga os passos na página Download para baixar o Cumulus Linux para a versão do software ONTAP que você está instalando.
   b. O RCF apropriado está disponível na "*NVIDIA Cluster e switches de armazenamento*"página. Siga os passos na página de transferência para transferir o RCF correto para a versão do software ONTAP que está a instalar.

Etapa 2: Configurar portas e cabeamento

Cumulus Linux 4.4.3

1. No novo switch nsw2, faça login como administrador e encerre todas as portas que serão conetadas às interfaces do cluster de nós (portas swp1 a swp14).

   As LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

   ```
   cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@nsw2:~$ net pending
   cumulus@nsw2:~$ net commit
   ```

2. Desativar a reversão automática nos LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert false`

   ```
   cluster1::*> network interface modify -vserver Cluster -lif * -auto
   -revert false

   Warning: Disabling the auto-revert feature of the cluster logical
   interface may effect the availability of your cluster network. Are
   you sure you want to continue? {y|n}: y
   ```

3. Verifique se todos os LIFs do cluster têm a reversão automática desabilitada:

   `net interface show -vserver Cluster -fields auto-revert`

4. Desligue as portas ISL swp15 e swp16 no interrutor SN2100 SW1.

   ```
   cumulus@sw1:~$ net add interface swp15-16 link down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

5. Remova todos os cabos do switch SN2100 SW1 e conete-os às mesmas portas do switch SN2100 nsw2.
6. Abra as portas ISL swp15 e swp16 entre os switches SW1 e nsw2.

   Os seguintes comandos ativam as portas ISL swp15 e swp16 no interrutor SW1:

   ```
   cumulus@sw1:~$ net del interface swp15-16 link down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

   O exemplo a seguir mostra que as portas ISL estão acima no interrutor SW1:

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP            Summary
-----  -----------  ----  -----  ----------  --------------
----------------------
...
...
UP     swp15        100G  9216   BondMember  nsw2 (swp15)    Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  nsw2 (swp16)    Master:
cluster_isl(UP)
```

O exemplo a seguir mostra que as portas ISL estão acima no interrutor nsw2:

```
cumulus@nsw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP            Summary
-----  -----------  ----  -----  ----------  -------------
-----------------------
...
...
UP     swp15        100G  9216   BondMember  sw1 (swp15)     Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)     Master:
cluster_isl(UP)
```

7. Verifique se a porta `e3b` está ativa em todos os nós:

   `network port show -ipspace Cluster`

   A saída deve ser semelhante ao seguinte:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                            Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- ------------
-------- -------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false


Node: node2

Ignore
                                                            Speed(Mbps)
Health    Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status    Status
--------- ------------ ---------------- ---- ----- -----------
--------- -------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false
```

8. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp3          -
node2      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp4          -
```

9. Verifique se todas as portas do cluster de nós estão ativas:

   `net show interface`

```
cumulus@nsw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

10. Verifique se ambos os nós têm uma conexão com cada switch:

    `net show lldp`

    O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  nsw2               swp15
swp16      100G   BondMember  nsw2               swp16


cumulus@nsw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1                e3b
swp4       100G   Trunk/L2    node2                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

11. Ativar a reversão automática nos LIFs do cluster:

    ```
    cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
    true
    ```

12. No switch nsw2, abra as portas conetadas às portas de rede dos nós.

    ```
    cumulus@nsw2:~$ net del interface swp1-14 link down
    cumulus@nsw2:~$ net pending
    cumulus@nsw2:~$ net commit
    ```

13. Exibir informações sobre os nós em um cluster:

    ```
    cluster show
    ```

    Este exemplo mostra que a integridade do nó para node1 e node2 neste cluster é verdadeira:

    ```
    cluster1::*> cluster show

    Node          Health  Eligibility
    ------------- ------- ------------
    node1         true    true
    node2         true    true
    ```

14. Verifique se todas as portas de cluster físico estão ativas:

```
network port show ipspace Cluster
```

```
cluster1::*> network port show -ipspace Cluster

Node node1
Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e3a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e3b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e3a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up    9000  auto/10000
healthy  false
```

Cumulus Linux 5.x

1. No novo switch nsw2, faça login como administrador e encerre todas as portas que serão conetadas às interfaces do cluster de nós (portas swp1 a swp14).

   As LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

   ```
   cumulus@nsw2:~$ nv set interface swp15-16 link state down
   cumulus@nsw2:~$ nv config apply
   ```

2. Desativar a reversão automática nos LIFs do cluster:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false

Warning: Disabling the auto-revert feature of the cluster logical
interface may effect the availability of your cluster network. Are
you sure you want to continue? {y|n}: y
```

3. Verifique se todos os LIFs do cluster têm a reversão automática desabilitada:

   `network interface show -vserver Cluster -fields auto-revert`

4. Desligue as portas ISL swp15 e swp16 no interrutor SN2100 SW1.

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

5. Remova todos os cabos do switch SN2100 SW1 e conete-os às mesmas portas do switch SN2100 nsw2.
6. Abra as portas ISL swp15 e swp16 entre os switches SW1 e nsw2.

   Os seguintes comandos ativam as portas ISL swp15 e swp16 no interrutor SW1:

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

   O exemplo a seguir mostra que as portas ISL estão acima no interrutor SW1:

```
cumulus@sw1:~$ nv show interface

State  Name         Spd   MTU    Mode        LLDP            Summary
-----  -----------  ----  -----  ----------  --------------
----------------------
...
...
UP     swp15        100G  9216   BondMember  nsw2 (swp15)    Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  nsw2 (swp16)    Master:
cluster_isl(UP)
```

   O exemplo a seguir mostra que as portas ISL estão acima no interrutor nsw2:

```
cumulus@nsw2:~$ nv show interface

State  Name          Spd   MTU    Mode         LLDP            Summary
-----  ------------  ----  -----  ----------  -------------
-----------------------
...
...
UP     swp15         100G  9216   BondMember  sw1 (swp15)     Master:
cluster_isl(UP)
UP     swp16         100G  9216   BondMember  sw1 (swp16)     Master:
cluster_isl(UP)
```

7. Verifique se a porta `e3b` está ativa em todos os nós:

   `network port show -ipspace Cluster`

   A saída deve ser semelhante ao seguinte:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- ------------
-------- -------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false


Node: node2

Ignore
                                                  Speed(Mbps)
Health    Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status    Status
--------- ------------ ---------------- ---- ----- -----------
--------- -------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false
```

8. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp3          -
node2      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp4          -
```

9. Verifique se todas as portas do cluster de nós estão ativas:

   `nv show interface`

```
cumulus@nsw2:~$ nv show interface

State  Name          Spd   MTU    Mode        LLDP
Summary
-----  ------------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3          100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp4          100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp15         100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16         100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

10. Verifique se ambos os nós têm uma conexão com cada switch:

    `nv show interface lldp`

    O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cumulus@sw1:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  nsw2               swp15
swp16      100G   BondMember  nsw2               swp16


cumulus@nsw2:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1                e3b
swp4       100G   Trunk/L2    node2                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

11. Ativar a reversão automática nos LIFs do cluster:

    ```
    cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
    true
    ```

12. No switch nsw2, abra as portas conetadas às portas de rede dos nós.

    ```
    cumulus@nsw2:~$ nv set interface swp1-14 link state up
    cumulus@nsw2:~$ nv config apply
    ```

13. Exibir informações sobre os nós em um cluster:

    ```
    cluster show
    ```

    Este exemplo mostra que a integridade do nó para node1 e node2 neste cluster é verdadeira:

    ```
    cluster1::*> cluster show

    Node           Health  Eligibility
    -------------- ------- ------------
    node1          true    true
    node2          true    true
    ```

14. Verifique se todas as portas de cluster físico estão ativas:

    ```
    network port show ipspace Cluster
    ```

```
cluster1::*> network port show -ipspace Cluster

Node node1
Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e3a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e3b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e3a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up    9000  auto/10000
healthy  false
```

Etapa 3: Verifique a configuração

Cumulus Linux 4.4.3

1. Verifique se a rede do cluster está em bom estado.

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost      RemotePort
---------  -----  ----------  --------------  -----------
swp3       100G   Trunk/L2    node1           e3a
swp4       100G   Trunk/L2    node2           e3a
swp15      100G   BondMember  nsw2            swp15
swp16      100G   BondMember  nsw2            swp16
```

Cumulus Linux 5.x

1. Verifique se a rede do cluster está em bom estado.

```
cumulus@sw1:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost      RemotePort
---------  -----  ----------  --------------  -----------
swp3       100G   Trunk/L2    node1           e3a
swp4       100G   Trunk/L2    node2           e3a
swp15      100G   BondMember  nsw2            swp15
swp16      100G   BondMember  nsw2            swp16
```

1. altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os switches de cluster NVIDIA SN2100 por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

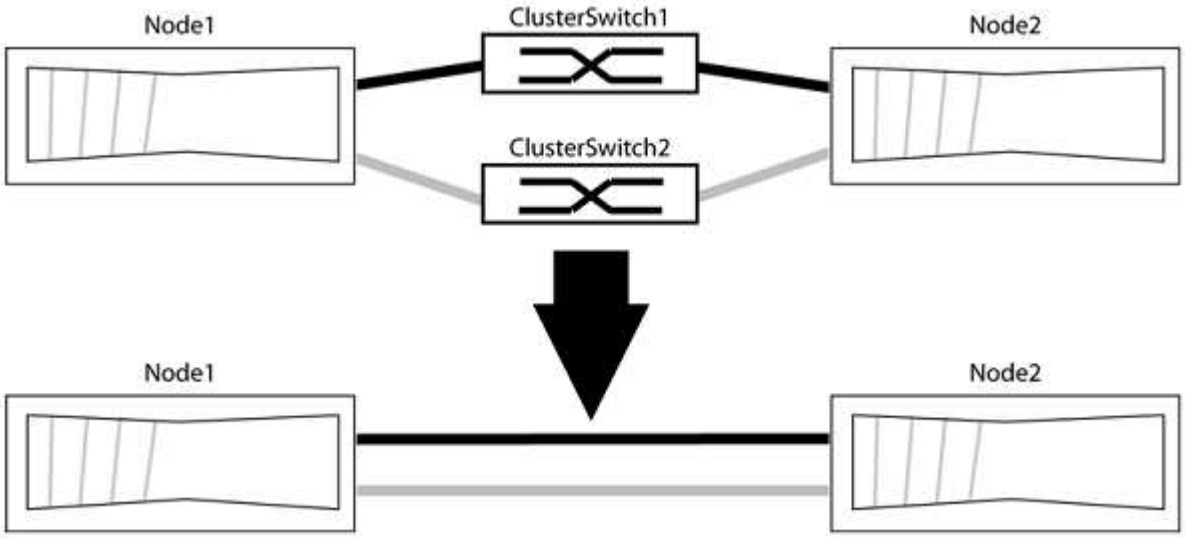
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

   `network options detect-switchless-cluster show`

   Mostrar exemplo

   A saída de exemplo a seguir mostra se a opção está ativada.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=<number_of_hours>h`

   `h`onde está a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico desta tarefa de manutenção para que possa suprimir a criação automática de casos durante a janela de manutenção.

   No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

   Mostrar exemplo

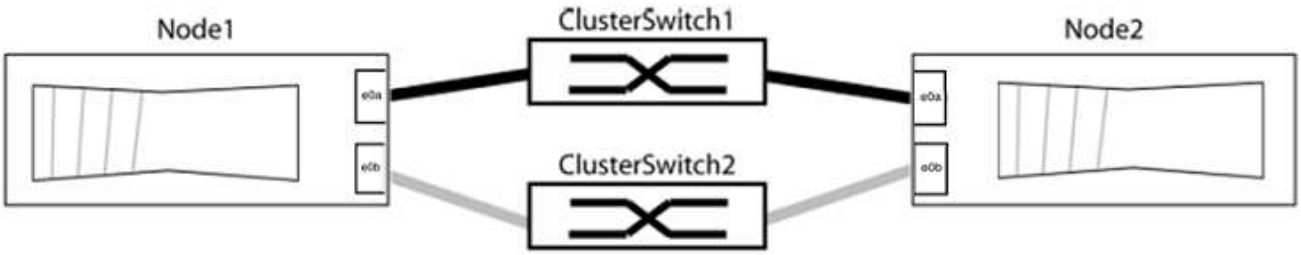
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-nvidia-sn2100/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar

usando portas de cluster diferentes porque variam de acordo com o sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

   Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

   ```
   network interface show -vserver Cluster -fields is-home
   ```

   Mostrar exemplo

   ```
   cluster::*> net int show -vserver Cluster -fields is-home
   (network interface show)
   vserver  lif          is-home
   -------- ------------ --------
   Cluster  node1_clus1  true
   Cluster  node1_clus2  true
   Cluster  node2_clus1  true
   Cluster  node2_clus2  true
   4 entries were displayed.
   ```

   Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

   ```
   network interface revert -vserver Cluster -lif *
   ```

4. Desativar a reversão automática para as LIFs do cluster:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

   ```
   network device-discovery show -port cluster_port
   ```

   A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

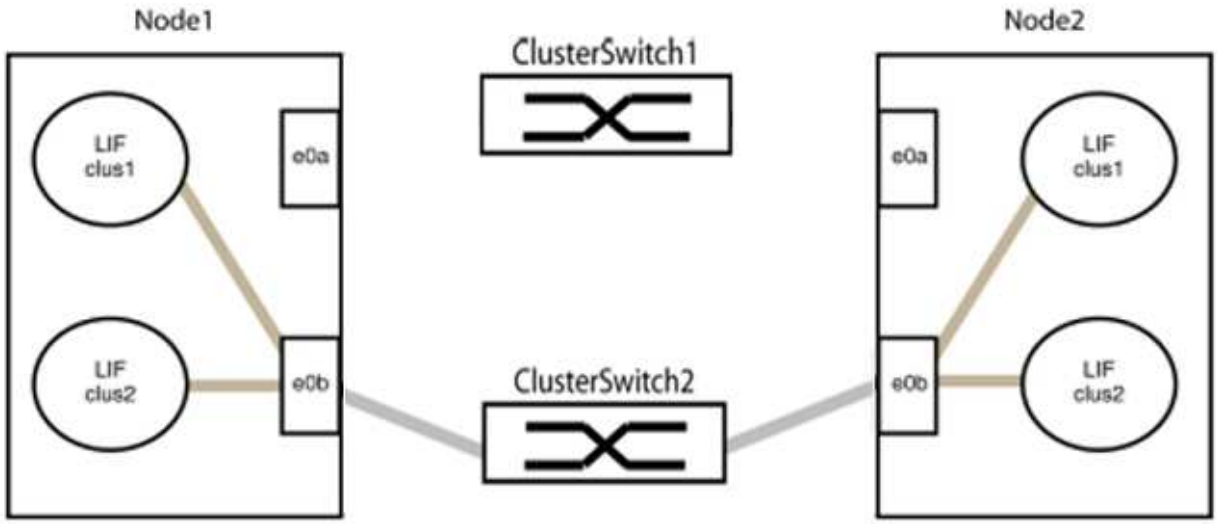
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

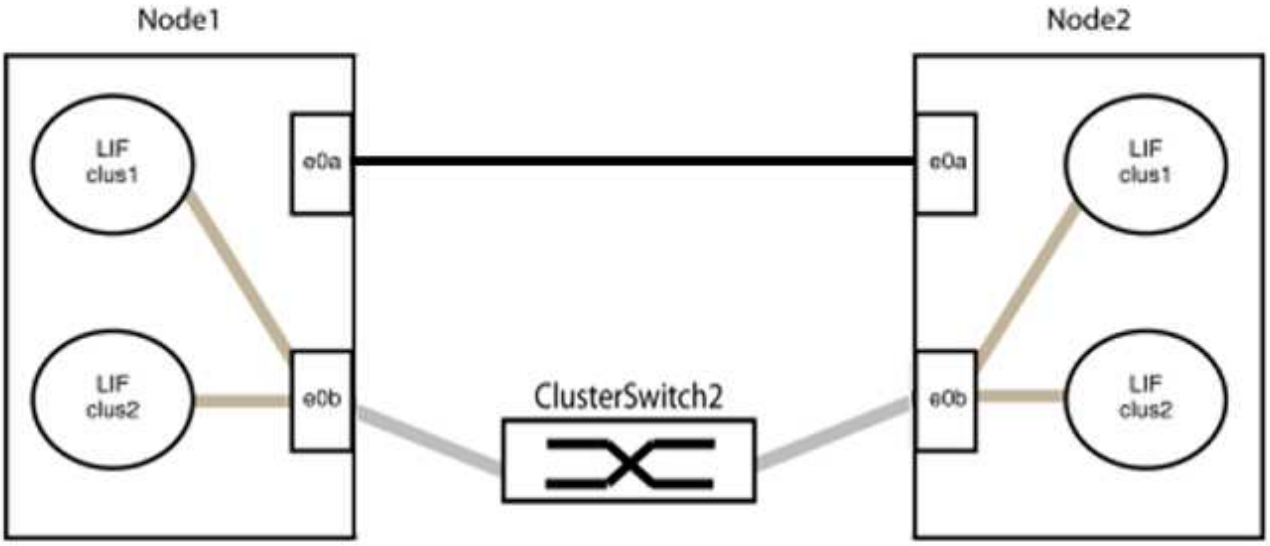
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

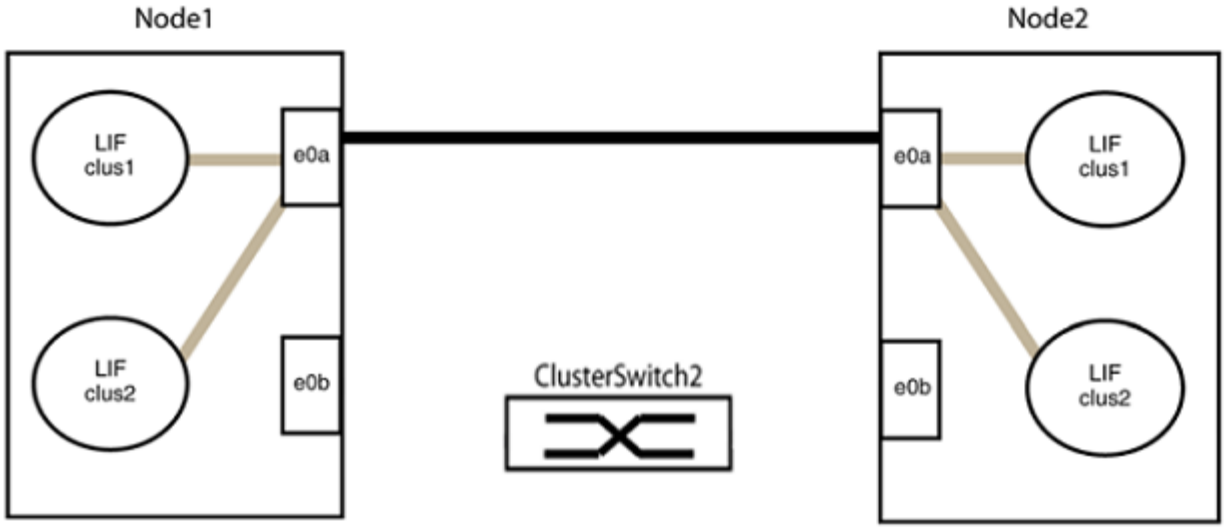
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

Interrutores de armazenamento

Cisco Nexus 9336CP-FX2 ou 9336CP-FX2BASE-T

Comece agora

Fluxo de trabalho de instalação e configuração para switches de armazenamento Cisco Nexus 9336C-FX2 9336C-FX2-T

Os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T fazem parte da plataforma Cisco Nexus 9000 e podem ser instalados em um gabinete de sistema NetApp .

O Cisco Nexus 9336C-FX2 (36 portas) é um switch de cluster/armazenamento/dados de alta densidade de portas. O Cisco Nexus 9336C-FX2-T (12 portas) é um switch de alto desempenho e baixa densidade de portas que suporta configurações de 10/25/40/100GbE.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches Cisco 9336C-FX2 e 9336C-FX2-T.

1. **"Revise os requisitos de configuração"**

Revise os requisitos de configuração para os switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

2. **"Revise os componentes e números de peça"**

Revise os componentes e números de peça dos switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

3. **"Revise a documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 9336C-FX2 e 9336C-FX2-T e o cluster ONTAP .

4. **"Revise os requisitos do Smart Call Home"**

Revise os requisitos do recurso Cisco Smart Call Home, usado para monitorar os componentes de hardware e software na sua rede.

5. **"Instale o hardware"**

Instale o hardware do switch.

6. **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalação e manutenção dos switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de revisar a configuração e os requisitos de rede.

Suporte à ONTAP

ONTAP 9.9,1 e posterior

A partir do ONTAP 9.9,1, você pode usar os switches Cisco Nexus 9336C-FX2 para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhado.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

> O monitor de integridade do switch Ethernet não suporta ONTAP 9.13.1P8 e anteriores e 9.14.1P3 e anteriores ou NX-os versão 10,3(4a)(M).

ONTAP 9.10.1 e posterior

Além disso, a partir do ONTAP 9.10.1, você pode usar os switches Cisco Nexus 9336C-FX2-T para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhada.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

Requisitos de configuração

Para a configuração, você precisa do número e tipo apropriados de cabos e conetores de cabo para seus switches.

Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para o tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700s, a interface e0M utiliza uma porta Ethernet dedicada.
- Consulte a "Hardware Universe" para obter as informações mais recentes.

Para obter mais informações sobre a configuração inicial do switch, consulte o seguinte guia: "Guia de instalação e atualização do Cisco Nexus 9336C-FX2".

O que vem a seguir

Depois de revisar os requisitos de configuração, você pode confirmar sua"componentes e números de peças"

.

Componentes e números de peça para switches de storage Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Para instalação e manutenção do switch de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de rever a lista de componentes e números de peça.

A tabela a seguir lista o número de peça e a descrição dos interrutores de armazenamento 9336C-FX2 e 9336C-FX2BASE-T, ventiladores e fontes de alimentação:

Número de peça	Descrição
X190200-CS-PE	Interrutor de cluster, N9336C 36Pt PTSX 10/25/40/100g
X190200-CS-PI	Comutador de cluster, N9336C 36Pt PSIN 10/25/40/100g
X190212-CS-PE	Interrutor de cluster, N9336C 12pt (9336C-FX2-T) PTSX 10/25/40/100g
X190212-CS-PI	Interrutor de cluster, N9336C 12pt (9336C-FX2-T) PSIN 10/25/40/100g
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 24 portas POD licença
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Kit de acessórios X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336CA AC 1100W PSU - fluxo de ar do escape lateral da porta
X-NXA-PAC-1100W-PI2	N9K-9336CA AC 1100W PSU - fluxo de ar de entrada lateral da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, fluxo de ar do escape lateral da porta
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, fluxo de ar de admissão do lado da porta

Licenças Cisco Smart somente para portas 9336C-FX2-T

Para ativar mais de 12 portas em seu switch de armazenamento Cisco Nexus 9336C-FX-T, você deve comprar uma licença Cisco Smart. As licenças inteligentes da Cisco são gerenciadas por meio de contas inteligentes da Cisco.

1. Crie uma nova conta Smart, se necessário. "Crie uma nova conta inteligente"Consulte para obter detalhes.
2. Solicitar acesso a uma conta inteligente existente. "Solicitar acesso a uma conta inteligente existente"Consulte para obter detalhes.

Depois de adquirir sua licença Smart, instale o RCF apropriado para habilitar e configurar todas as 36 portas disponíveis para uso.

O que vem a seguir

Depois de confirmar seus componentes e números de peça, revise o"documentação necessária" .

Requisitos de documentação para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalação e manutenção dos switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de revisar a documentação específica do switch e do controlador para configurar seus switches Cisco 9336-FX2 e o cluster ONTAP .

Documentação do switch

Para configurar os switches Cisco Nexus 9336C-FX2, você precisa da seguinte documentação na "Suporte para switches Cisco Nexus 9000 Series" página:

Título do documento	Descrição
Guia de Instalação de hardware da Série Nexus 9000	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
Guias de configuração do software de comutador da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
Guia de atualização e downgrade do software NX-os da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
Cisco Nexus 9000 Series NX-os Guia de Referência de comando	Fornece links para as várias referências de comando fornecidas pelo Cisco.
Cisco Nexus 9000 MIBs Referência	Descreve os arquivos MIB (Management Information base) para os switches Nexus 9000.
Nexus 9000 Series NX-os System Message Reference	Descreve as mensagens do sistema para os switches da série Cisco Nexus 9000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de lançamento do Cisco Nexus 9000 Series NX-os (escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 9000 Series.
Conformidade regulamentar e informações de segurança para a série Cisco Nexus 9000	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 9000.

Documentação de sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para sua versão do sistema operacional "ONTAP 9" .

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.
Documentação do ONTAP	Fornece informações detalhadas sobre todos os aspetos das versões do ONTAP.
"Hardware Universe"	Fornece informações de compatibilidade e configuração de hardware NetApp.

Kit de trilho e documentação do gabinete

Para instalar um switch Cisco 9336-FX2 em um gabinete NetApp, consulte a documentação de hardware a seguir.

Nome	Descrição
"Armário do sistema 42U, guia profundo"	Descreve as FRUs associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição da FRU.
"Instale um switch Cisco 9336-FX2 em um gabinete NetApp"	Descreve como instalar um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp de quatro colunas.

Requisitos para Smart Call Home

Para usar o Smart Call Home, você deve configurar um switch de rede de cluster para se comunicar por e-mail com o sistema Smart Call Home. Além disso, você pode opcionalmente configurar seu switch de rede de cluster para aproveitar o recurso de suporte Smart Call Home incorporado da Cisco.

O Smart Call Home monitora os componentes de hardware e software na sua rede. Quando ocorre uma configuração crítica do sistema, ele gera uma notificação por e-mail e envia um alerta para todos os destinatários configurados no seu perfil de destino.

Antes de usar o Smart Call Home, esteja ciente dos seguintes requisitos:

- Um servidor de e-mail deve estar no lugar.
- O switch deve ter conetividade IP com o servidor de e-mail.
- É necessário configurar o nome do contacto (contacto do servidor SNMP), o número de telefone e as informações do endereço da rua. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID de CCO deve ser associado a um contrato de serviço Cisco SMARTnet apropriado para a sua empresa.

- O Serviço SMARTnet da Cisco deve estar em vigor para que o dispositivo seja registrado.

O "Site de suporte da Cisco" contém informações sobre os comandos para configurar Smart Call Home.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalar e configurar o hardware dos switches de armazenamento 9336C-FX2 e 9336C-FX2-T, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2. **"Instale o interrutor"**

Instale os switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

3. **"Instale o interrutor em um gabinete NetApp"**

Instale os switches 9336C-FX2 e 9336C-FX2-T e o painel de passagem em um gabinete NetApp , conforme necessário.

Complete a Planilha de cabeamento do Cisco Nexus 9336C-FX2 ou 9336C-FX2-T.

Se você quiser documentar as plataformas suportadas, baixe um PDF desta página e complete a Planilha de cabeamento.

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

- Planilha de cabeamento de amostra 9336C-FX2
- Folha de cálculo de cabeamento em branco 9336C-FX2
- Folha de cálculo de cabeamento de amostra 9336C-FX2BASE-T (12 portas)
- Folha de cálculo de cabeamento em branco 9336C-FX2BASE-T (12 portas)

Planilha de cabeamento de amostra 9336C-FX2

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
1	4x100GbE nó 1	1	4x100GbE nó 1
2	4x100GbE nó 2	2	4x100GbE nó 2
3	4x100GbE nó 3	3	4x100GbE nó 3
4	4x100GbE nó 4	4	4x100GbE nó 4
5	4x100GbE nó 5	5	4x100GbE nó 5
6	4x100GbE nó 6	6	4x100GbE nó 6
7	4x100GbE nó 7	7	4x100GbE nó 7
8	4x100GbE nó 8	8	4x100GbE nó 8
9	4x100GbE nó 9	9	4x100GbE nó 9
10	4x100GbE nó 10	10	4x100GbE nó 10
11	4x100GbE nó 11	11	4x100GbE nó 11
12	4x100GbE nó 12	12	4x100GbE nó 12
13	4x100GbE nó 13	13	4x100GbE nó 13
14	4x100GbE nó 14	14	4x100GbE nó 14
15	4x100GbE nó 15	15	4x100GbE nó 15
16	4x100GbE nó 16	16	4x100GbE nó 16
17	4x100GbE nó 17	17	4x100GbE nó 17
18	4x100GbE nó 18	18	4x100GbE nó 18
19	4x100GbE nó 19	19	4x100GbE nó 19
20	4x100GbE nó 20	20	4x100GbE nó 20
21	4x100GbE nó 21	21	4x100GbE nó 21
22	4x100GbE nó 22	22	4x100GbE nó 22

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
23	4x100GbE nó 23	23	4x100GbE nó 23
24	4x100GbE nó 24	24	4x100GbE nó 24
25	4x100GbE nó 25	25	4x100GbE nó 25
26	4x100GbE nó 26	26	4x100GbE nó 26
27	4x100GbE nó 27	27	4x100GbE nó 27
28	4x100GbE nó 28	28	4x100GbE nó 28
29	4x100GbE nó 29	29	4x100GbE nó 29
30	4x100GbE nó 30	30	4x100GbE nó 30
31	4x100GbE nó 31	31	4x100GbE nó 31
32	4x100GbE nó 32	32	4x100GbE nó 32
33	4x100GbE nó 33	33	4x100GbE nó 33
30	4x100GbE nó 30	30	4x100GbE nó 33
34	4x100GbE nó 34	34	4x100GbE nó 34
35	4x100GbE nó 35	35	4x100GbE nó 35
36	4x100GbE nó 36	36	4x100GbE nó 36

Folha de cálculo de cabeamento em branco 9336C-FX2

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A seção *conexões de cluster suportadas* da "Hardware Universe" define as portas de cluster usadas pela plataforma.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
1		1	
2		2	
3		3	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

Folha de cálculo de cabeamento de amostra 9336C-FX2BASE-T (12 portas)

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta
1	4x100GbE nó 1	1	4x100GbE nó 1
2	4x100GbE nó 2	2	4x100GbE nó 2
3	4x100GbE nó 3	3	4x100GbE nó 3
4	4x100GbE nó 4	4	4x100GbE nó 4
5	4x100GbE nó 5	5	4x100GbE nó 5
6	4x100GbE nó 6	6	4x100GbE nó 6
7	4x100GbE nó 7	7	4x100GbE nó 7

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
8	4x100GbE nó 8	8	4x100GbE nó 8
9	4x100GbE nó 9	9	4x100GbE nó 9
10	4x100GbE nó 10	10	4x100GbE nó 10
11 embora 36	Requer licença	11 a 36	Requer licença

Folha de cálculo de cabeamento em branco 9336C-FX2BASE-T (12 portas)

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 a 36	Requer licença	11 a 36	Requer licença

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você"instalar o interruptor" .

Instalar os switches de armazenamento 9336C-FX2 e 9336C-FX2-T

Siga este procedimento para instalar os switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões de NX-os e arquivo de configuração de referência (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- "fichas de trabalho de cablagem"Concluído .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- Documentação necessária do interrutor. Consulte "Documentação necessária" para obter mais informações.

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o seu…	Então…
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte "Instale o interrutor no gabinete do NetApp" para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.

O que se segue?

Opcionalmente, você pode"Instale um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp" . Caso contrário, vá para"configurar o switch" .

Instalar switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T em um gabinete NetApp

Dependendo da sua configuração, pode ser necessário instalar os switches Cisco Nexus 9336C-FX2 9336C-FX2-T e o painel de passagem em um gabinete NetApp . Suportes padrão estão incluídos com o interruptor.

Antes de começar

Certifique-se de que tem o seguinte:

- Para cada interrutor, você deve fornecer os oito parafusos 10-32 ou 12-24 e porcas de grampo para montar os suportes e trilhos deslizantes nos postes dianteiros e traseiros do gabinete.
- Você deve usar o kit de trilho padrão Cisco para instalar o switch em um gabinete NetApp.

> Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

Documentação necessária

Reveja os requisitos iniciais de preparação, o conteúdo do kit e as precauções de segurança no "Guia de instalação de hardware do Cisco Nexus 9000 Series".

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

   O kit de painel de passagem está disponível na NetApp (código de peça X8784-R6).

   O kit do painel de passagem do NetApp contém o seguinte hardware:

   - Um painel obturador de passagem
   - Quatro parafusos 10-32 x .75
   - Quatro porcas de freio 10-32

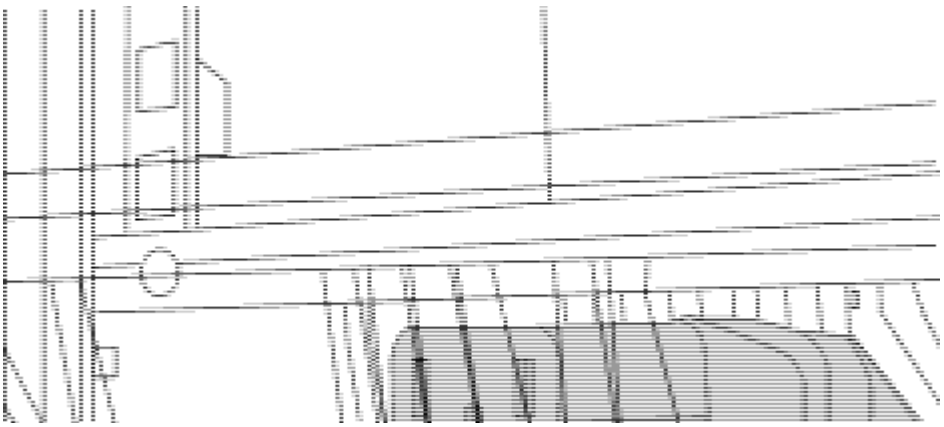
     i. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

     Neste procedimento, o painel obturador será instalado em U40.

     ii. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

     iii. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

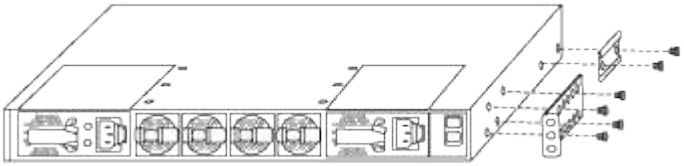
     iv. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.



(1) conetor fêmea do cabo de ligação em ponte.

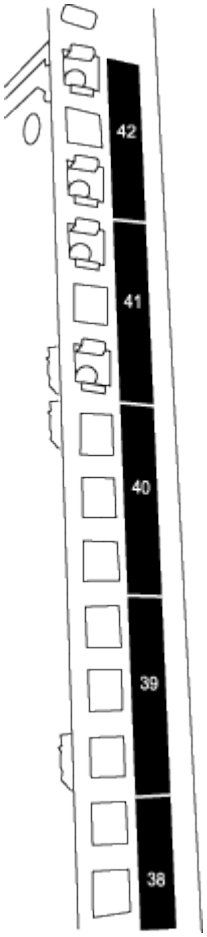
2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.
   a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do

ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.



b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.
c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.
d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.

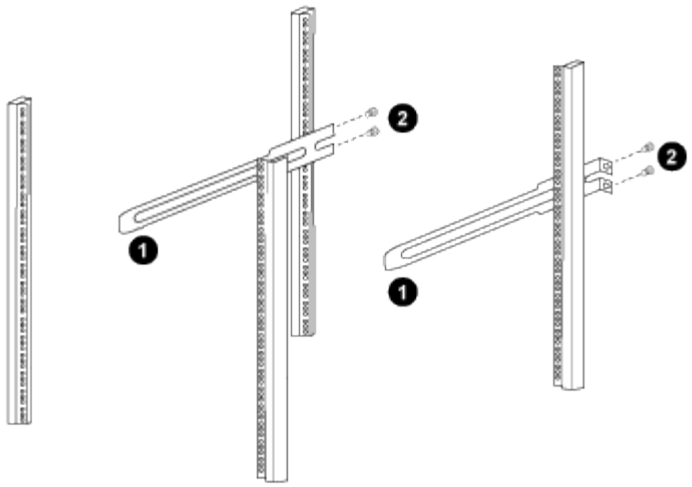
3. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



Os dois interrutores 9336C-FX2 sempre serão montados no topo 2U do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no gabinete.

a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



(1) enquanto desliza suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.

(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

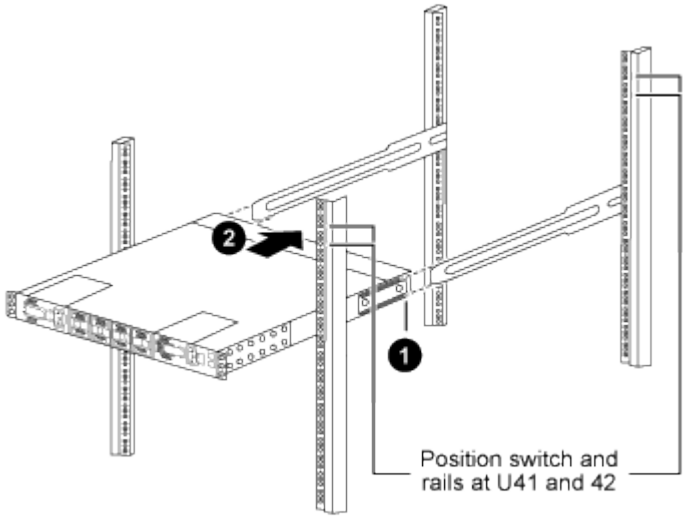
a. Repita o passo 4a para a coluna traseira do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

5. Instale o interrutor no gabinete.

Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

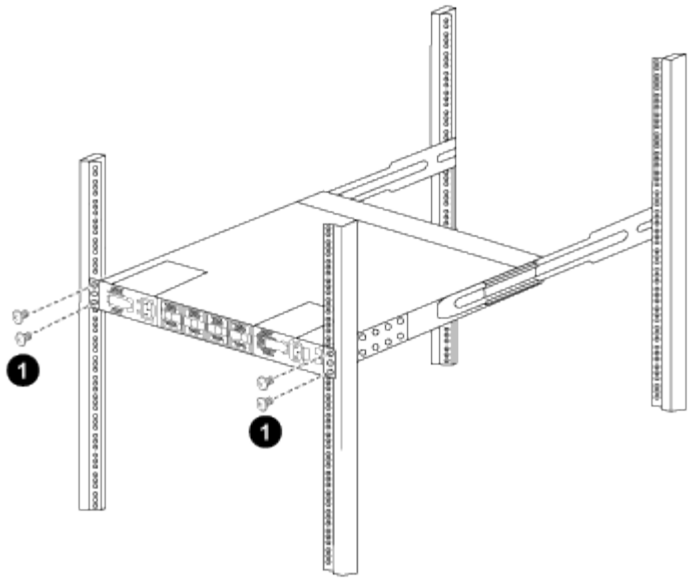
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário manter a frente do segundo interrutor durante o processo de instalação.

6. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
7. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

8. Conete a porta de gerenciamento de cada switch 9336C-FX2 a um dos switches de gerenciamento (se solicitado) ou conete-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

O que vem a seguir

Depois de instalar os switches no gabinete NetApp , você"configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T" .

Configurar o software

Fluxo de trabalho de instalação de software para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalar e configurar o software para os switches de armazenamento Cisco Nexus

9336C-FX2 e 9336C-FX2-T, siga estas etapas:

1. **"Configure o interrutor"**

Configure os switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

2. **"Prepare-se para instalar o software NX-os e o RCF"**

O software Cisco NX-OS e os arquivos de configuração de referência (RCFs) devem ser instalados nos switches de armazenamento Cisco 9336C-FX2 e 9336C-FX2-T.

3. **"Instale ou atualize o software NX-os"**

Baixe e instale ou atualize o software NX-OS nos switches de armazenamento Cisco 9336C-FX2 e 9336C-FX2-T.

4. **"Instale ou atualize o RCF"**

Instale ou atualize o RCF após configurar os switches Cisco 9336C-FX2 e 9336C-FX2-T pela primeira vez. Você também pode usar este procedimento para atualizar sua versão do RCF.

5. **"Verifique a configuração do SSH"**

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

6. **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações dos switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

Configurar os switches de armazenamento 9336C-FX2 e 9336C-FX2-T

Siga este procedimento para configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões de NX-os e arquivo de configuração de referência (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- "fichas de trabalho de cablagem"Concluído .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual

do software NX-os, mas não têm os RCFs carregados.

- Documentação necessária do interrutor. Consulte "Documentação necessária" para obter mais informações.

Passos

1. Execute uma configuração inicial dos switches de rede do cluster.

   Forneça respostas aplicáveis às seguintes perguntas de configuração inicial ao inicializar o switch pela primeira vez. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Aviso	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com **sim**. A predefinição é não
Pretende aplicar o padrão de palavra-passe seguro? (sim/não)	Responda com **sim**. O padrão é sim.
Introduza a palavra-passe para admin.	A senha padrão é '"admin"'; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Pretende introduzir a caixa de diálogo de configuração básica? (sim/não)	Responda com **sim** na configuração inicial do comutador.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em administradores alternativos. O padrão é **não**.
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com **não**. A predefinição é não
Configurar string de comunidade SNMP de leitura-escrita? (sim/não)	Responda com **não**. A predefinição é não
Introduza o nome do interrutor.	O nome do switch está limitado a 63 carateres alfanuméricos.
Continuar com a configuração de gerenciamento fora da banda (mgmt0)? (sim/não)	Responda com **yes** (o padrão) nesse prompt. No prompt mgmt0 IPv4 address:, insira seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com **sim**. No endereço IPv4 do prompt default-gateway:, digite seu default_gateway.
Configurar opções IP avançadas? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço telnet? (sim/não)	Responda com **não**. A predefinição é não

Aviso	Resposta
Ativar o serviço SSH? (sim/não)	Responda com **sim**. O padrão é sim. O SSH é recomendado ao usar o Ethernet Switch Health Monitor (CSHM) para seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Introduza o tipo de chave SSH que pretende gerar (dsa/rsa/rsa1).	O padrão é **rsa**.
Introduza o número de bits de chave (1024-2048).	Introduza o número de bits de chave de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com **não**. A predefinição é não
Configurar camada de interface padrão (L3/L2)	Responda com **L2**. A predefinição é L2.
Configurar o estado predefinido da interface da porta do switch (shut/noshut)	Responda com **noshut**. O padrão é noshut.
Configurar o perfil do sistema CoPP (strict/moderate/lenient/dense)	Responda com **strict**. O padrão é rigoroso.
Pretende editar a configuração? (sim/não)	Você deve ver a nova configuração neste momento. Reveja e faça as alterações necessárias à configuração que acabou de introduzir. Responda com **no** no prompt se você estiver satisfeito com a configuração. Responda com **yes** se quiser editar as configurações.
Utilizar esta configuração e guardá-la? (sim/não)	Responda com **yes** para salvar a configuração. Isto atualiza automaticamente as imagens do Kickstart e do sistema. Se você não salvar a configuração nesta fase, nenhuma das alterações entrará em vigor na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração que você fez no visor que aparece no final da configuração e certifique-se de salvar a configuração.
3. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software suportada pelo NetApp para os switches a partir da "Transferência do software Cisco" página.

O que se segue?

Depois de configurar seus switches, você"prepare-se para instalar o software NX-OS e RCF" .

Prepare-se para instalar ou atualizar o software NX-os e o RCF

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01 e cluster1-02.
- Os nomes de LIF de cluster são 02-01_clus1 e cluster1-01_clus2 para cluster1-01 e cluster1-02_clus1 e cluster1-02_clus2 para cluster1-cluster1.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   network device-discovery show -protocol lldp
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/lldp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/lldp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C

4 entries were displayed.
```

4. Verifique o status administrativo ou operacional de cada interface de cluster.
   a. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- ------------
------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- ------------
------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false

4 entries were displayed.
```

b. Exibir informações sobre os LIFs:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2024 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2024 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2024 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2024 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o comando de reversão automática está ativado em todas as LIFs do cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

O que se segue?

Depois de se preparar para instalar o software NX-OS e o RCF, você"instalar ou atualizar o software NX-OS" .

Instale ou atualize o software NX-os

Siga este procedimento para instalar o software NX-OS nos switches Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar, conclua o procedimento em "Prepare-se para instalar o NX-os e o RCF".

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- "Página do switch Ethernet Cisco"

  Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

- "Guias de atualização e downgrade de software"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

- "Atualização do Cisco Nexus 9000 e 3000 e Matriz ISSU"

  Fornece informações sobre atualização/downgrade disruptiva para o software Cisco NX-os em switches Nexus 9000 Series com base em suas versões atuais e de destino.

Na página, selecione **Atualização disruptiva** e selecione sua versão atual e liberação de destino na lista suspensa.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-03_clus1 , cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.
- O `cluster1::*>` prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch pode alcançar o servidor no endereço IP 172.19.2.1:

   ```
   cs2# ping 172.19.2.1 VRF management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Copie o software NX-os e as imagens EPLD para o switch Nexus 9336C-FX2.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.5.bin  /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time:  05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 02:28:31]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS



Compatibility check is done:
Module  Bootable  Impact          Install-type  Reason
------  --------  --------------- ------------  ---------
  1     yes       Disruptive      Reset         Default upgrade is
not hitless



Images will be upgraded according to following table:

Module   Image    Running-Version(pri:alt)                 New-
Version         Upg-Required
-------  -------- ---------------------------------------
-------------------- ------------
  1      nxos     9.3(4)                                   9.3(5)
yes
  1      bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)      yes
```

```
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.
```

9. Verifique a nova versão do software NX-os depois que o switch reiniciar:

   `show version`

Mostrar exemplo

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.3(5)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

10. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x17
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2

cs2# 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.
```

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

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x19
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
```

12. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -role cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
```

```
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

13. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

14. Repita os passos 6 a 13 para instalar o software NX-os no interrutor CS1.
15. Ative a reversão automática nos LIFs do cluster.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

16. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que se segue?

Depois de instalar ou atualizar o software NX-OS, você"instalar ou atualizar o RCF" .

Instale ou atualize o ficheiro de configuração de referência

Você instala o arquivo de configuração de referência (RCF) após configurar os switches de armazenamento Nexus 9336C-FX2 e 9336C-FX2-T pela primeira vez.

Consulte o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de

interconexão Cisco, mantendo a conetividade remota"para obter mais informações ao instalar o RCF.

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma ligação de consola ao interrutor. A conexão do console é opcional se você tiver acesso remoto ao switch.
- O switch CS1 e o switch CS2 são ativados e a configuração inicial do switch está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão NX-os pretendida foi instalada.
- As portas do cluster de nós do ONTAP não estão conetadas.

Passo 1: Instale o RCF nos interrutores

1. Faça login no switch CS1 usando SSH ou usando um console serial.
2. Copie o RCF para o flash de inicialização do switch CS1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referência de comando Cisco Nexus 9000 Series NX-os".

   Mostrar exemplo

   Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS1:

   ```
   cs1# copy tftp: bootflash: vrf management
   Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
   Enter hostname for the tftp server: 172.22.201.50
   Trying to connect to tftp server......Connection to Server
   Established.
   TFTP get operation was successful
   Copy complete, now saving to disk (please wait)...
   ```

3. Aplique o RCF baixado anteriormente ao flash de inicialização.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referência de comando Cisco Nexus 9000 Series NX-os".

   Mostrar exemplo

   Este exemplo mostra o RCF `Nexus_9336C_RCF_v1.6-Storage.txt` a ser instalado no interrutor CS1:

   ```
   cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
   commands
   ```

4. Examine a saída do banner a partir do `show banner motd` comando. Deve ler e seguir estas instruções para garantir a configuração e funcionamento corretos do interrutor.

Mostrar exemplo

```
cs1# show banner motd

**********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch    : Nexus N9K-C9336C-FX2
* Filename  : Nexus_9336C_RCF_v1.6-Storage.txt
* Date      : 10-23-2020
* Version   : v1.6
*
* Port Usage : Storage configuration
* Ports  1-36: 100GbE Controller and Shelf Storage Ports
**********************************************************************
**********
```

5. Verifique se o RCF é a versão mais recente correta:

`show running-config`

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.
7. Depois de verificar se as versões RCF e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

```
cs1# copy running-config startup-config
[########################################] 100% Copy complete
```

8. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

   Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

10. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

11. Emitir o `write erase` comando para apagar a configuração salva atual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

12. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Interrutor de reinicialização CS1.

```
cs1# reload

This command will reboot the system. (y/n)? [n] y
```

14. Repita os passos 1 a 13 no switch cs2.
15. Conecte as portas do cluster de todos os nós do cluster ONTAP aos switches CS1 e CS2.

Etapa 2: Verifique as conexões do interrutor

1. Verifique se as portas do switch conetadas às portas do cluster estão **up**.

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
mgmt0  --           up     <mgmt ip address>
1000    1500
Eth1/11         1       eth  trunk  up      none
100G(D) --
Eth1/12         1       eth  trunk  up      none
100G(D) --
Eth1/13         1       eth  trunk  up      none
100G(D) --
Eth1/14         1       eth  trunk  up      none
100G(D) --
Eth1/15         1       eth  trunk  up      none
100G(D) --
Eth1/16         1       eth  trunk  up      none
100G(D) --
Eth1/17         1       eth  trunk  up      none
100G(D) --
Eth1/18         1       eth  trunk  up      none
100G(D) --
Eth1/23         1       eth  trunk  up      none
100G(D) --
Eth1/24         1       eth  trunk  up      none
100G(D) --
Eth1/25         1       eth  trunk  up      none
100G(D) --
Eth1/26         1       eth  trunk  up      none
100G(D) --
Eth1/27         1       eth  trunk  up      none
100G(D) --
Eth1/28         1       eth  trunk  up      none
100G(D) --
Eth1/29         1       eth  trunk  up      none
100G(D) --
Eth1/30         1       eth  trunk  up      none
100G(D) --
```

2. Verifique se os nós de cluster estão em suas VLANs de cluster corretas usando os seguintes comandos:

   `show vlan brief`

   `show interface trunk`

Mostrar exemplo

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Po999
30   VLAN0030                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9, Eth1/10,
Eth1/11
                                                 Eth1/12, Eth1/13,
Eth1/14
                                                 Eth1/15, Eth1/16,
Eth1/17
                                                 Eth1/18, Eth1/19,
Eth1/20
                                                 Eth1/21, Eth1/22,
Eth1/23
                                                 Eth1/24, Eth1/25,
Eth1/26
                                                 Eth1/27, Eth1/28,
Eth1/29
                                                 Eth1/30, Eth1/31,
Eth1/32
                                                 Eth1/33, Eth1/34,
Eth1/35
                                                 Eth1/36

cs1# show interface trunk

--------------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
--------------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
```

```
Eth1/9        1       trunking      --
Eth1/10       1       trunking      --
Eth1/11       1       trunking      --
Eth1/12       1       trunking      --
Eth1/13       1       trunking      --
Eth1/14       1       trunking      --
Eth1/15       1       trunking      --
Eth1/16       1       trunking      --
Eth1/17       1       trunking      --
Eth1/18       1       trunking      --
Eth1/19       1       trunking      --
Eth1/20       1       trunking      --
Eth1/21       1       trunking      --
Eth1/22       1       trunking      --
Eth1/23       1       trunking      --
Eth1/24       1       trunking      --
Eth1/25       1       trunking      --
Eth1/26       1       trunking      --
Eth1/27       1       trunking      --
Eth1/28       1       trunking      --
Eth1/29       1       trunking      --
Eth1/30       1       trunking      --
Eth1/31       1       trunking      --
Eth1/32       1       trunking      --
Eth1/33       1       trunking      --
Eth1/34       1       trunking      --
Eth1/35       1       trunking      --
Eth1/36       1       trunking      --

--------------------------------------------------------------------------
------------
Port          Vlans Allowed on Trunk
--------------------------------------------------------------------------
------------
Eth1/1        30
Eth1/2        30
Eth1/3        30
Eth1/4        30
Eth1/5        30
Eth1/6        30
Eth1/7        30
Eth1/8        30
Eth1/9        30
Eth1/10       30
Eth1/11       30
Eth1/12       30
```

```
Eth1/13       30
Eth1/14       30
Eth1/15       30
Eth1/16       30
Eth1/17       30
Eth1/18       30
Eth1/19       30
Eth1/20       30
Eth1/21       30
Eth1/22       30
Eth1/23       30
Eth1/24       30
Eth1/25       30
Eth1/26       30
Eth1/27       30
Eth1/28       30
Eth1/29       30
Eth1/30       30
Eth1/31       30
Eth1/32       30
Eth1/33       30
Eth1/34       30
Eth1/35       30
Eth1/36       30

--------------------------------------------------------------------------------
------------
Port          Vlans Err-disabled on Trunk
--------------------------------------------------------------------------------
------------
Eth1/1        none
Eth1/2        none
Eth1/3        none
Eth1/4        none
Eth1/5        none
Eth1/6        none
Eth1/7        none
Eth1/8        none
Eth1/9        none
Eth1/10       none
Eth1/11       none
Eth1/12       none
Eth1/13       none
Eth1/14       none
Eth1/15       none
Eth1/16       none
```

```
Eth1/17       none
Eth1/18       none
Eth1/19       none
Eth1/20       none
Eth1/21       none
Eth1/22       none
Eth1/23       none
Eth1/24       none
Eth1/25       none
Eth1/26       none
Eth1/27       none
Eth1/28       none
Eth1/29       none
Eth1/30       none
Eth1/31       none
Eth1/32       none
Eth1/33       none
Eth1/34       none
Eth1/35       none
Eth1/36       none

--------------------------------------------------------------------------
------------
Port          STP Forwarding
--------------------------------------------------------------------------
------------
Eth1/1        none
Eth1/2        none
Eth1/3        none
Eth1/4        none
Eth1/5        none
Eth1/6        none
Eth1/7        none
Eth1/8        none
Eth1/9        none
Eth1/10       none
Eth1/11       30
Eth1/12       30
Eth1/13       30
Eth1/14       30
Eth1/15       30
Eth1/16       30
Eth1/17       30
Eth1/18       30
Eth1/19       none
Eth1/20       none
```

```
Eth1/21       none
Eth1/22       none
Eth1/23       30
Eth1/24       30
Eth1/25       30
Eth1/26       30
Eth1/27       30
Eth1/28       30
Eth1/29       30
Eth1/30       30
Eth1/31       none
Eth1/32       none
Eth1/33       none
Eth1/34       none
Eth1/35       none
Eth1/36       none

--------------------------------------------------------------------------------
Port          Vlans in spanning tree forwarding state and not pruned
--------------------------------------------------------------------------------
Eth1/1        Feature VTP is not enabled
none
Eth1/2        Feature VTP is not enabled
none
Eth1/3        Feature VTP is not enabled
none
Eth1/4        Feature VTP is not enabled
none
Eth1/5        Feature VTP is not enabled
none
Eth1/6        Feature VTP is not enabled
none
Eth1/7        Feature VTP is not enabled
none
Eth1/8        Feature VTP is not enabled
none
Eth1/9        Feature VTP is not enabled
none
Eth1/10       Feature VTP is not enabled
none
Eth1/11       Feature VTP is not enabled
30
Eth1/12       Feature VTP is not enabled
30
```

```
Eth1/13       Feature VTP is not enabled
30
Eth1/14       Feature VTP is not enabled
30
Eth1/15       Feature VTP is not enabled
30
Eth1/16       Feature VTP is not enabled
30
Eth1/17       Feature VTP is not enabled
30
Eth1/18       Feature VTP is not enabled
30
Eth1/19       Feature VTP is not enabled
none
Eth1/20       Feature VTP is not enabled
none
Eth1/21       Feature VTP is not enabled
none
Eth1/22       Feature VTP is not enabled
none
Eth1/23       Feature VTP is not enabled
30
Eth1/24       Feature VTP is not enabled
30
Eth1/25       Feature VTP is not enabled
30
Eth1/26       Feature VTP is not enabled
30
Eth1/27       Feature VTP is not enabled
30
Eth1/28       Feature VTP is not enabled
30
Eth1/29       Feature VTP is not enabled
30
Eth1/30       Feature VTP is not enabled
30
Eth1/31       Feature VTP is not enabled
none
Eth1/32       Feature VTP is not enabled
none
Eth1/33       Feature VTP is not enabled
none
Eth1/34       Feature VTP is not enabled
none
Eth1/35       Feature VTP is not enabled
none
```

```
Eth1/36       Feature VTP is not enabled
none
```

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

Passo 3: Configure o cluster do ONTAP

A NetApp recomenda que você use o Gerenciador de sistemas para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e configuração de cluster, incluindo a atribuição de um endereço IP de gerenciamento de nós, a inicialização do cluster, a criação de um nível local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Aceda a "Configure o ONTAP em um novo cluster com o Gerenciador do sistema" para obter instruções de configuração.

O que se segue?

Depois de instalar ou atualizar seu RCF, você"verificar a configuração SSH"

Verifique a configuração da SSH

Se você estiver usando os recursos CSHM (Ethernet Switch Health Monitor) e coleta de logs, verifique se as chaves SSH e SSH estão habilitadas nos switches de cluster.

Passos

1. Verifique se o SSH está ativado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verifique se as chaves SSH estão ativadas:

```
show ssh key
```

Mostrar exemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Ao ativar o FIPS, você deve alterar o número de bits para 256 na central usando o comando `ssh key ecdsa 256 force`. "Configurar a segurança da rede usando o FIPS"Consulte para obter mais detalhes.

O que se segue?

Depois de verificar sua configuração SSH, você"configurar monitoramento de integridade do switch" .

Redefinir os switches de armazenamento 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica

Para redefinir os switches de armazenamento 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica, você deve apagar as configurações dos switches 9336C-FX2 e 9336C-FX2-T.

Sobre esta tarefa

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

Passos

1. Apagar a configuração existente:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Recarregue o software do switch:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   O sistema é reinicializado e entra no assistente de configuração. Durante a inicialização, se você receber o prompt “Abortar provisionamento automático e continuar com a configuração normal? (sim/não)[n]”, você deve responder **sim** para prosseguir.

Substituir switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Você pode substituir switches Nexus 9336C-FX2 e 9336C-FX2-T defeituosos em uma rede de cluster. Este é um procedimento não disruptivo.

Antes de começar

Antes de instalar o software NX-OS e os RCFs nos switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de que:

- Seu sistema pode suportar switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T.
- Você consultou a tabela de compatibilidade do switch na página do switch Ethernet Cisco para as versões ONTAP, NX-os e RCF suportadas.
- Você se referiu ao software apropriado e aos guias de atualização disponíveis no site da Cisco.

Switches da série Cisco Nexus 3000:

- Você baixou os RCFs aplicáveis.
- A configuração de rede existente tem as seguintes caraterísticas:
  - A página de switches Ethernet Cisco tem as versões mais recentes de RCF e NX-os em seus switches.
  - A conetividade de gerenciamento deve existir em ambos os switches.
- O switch Cisco Nexus 9336C-FX2 de substituição tem as seguintes caraterísticas:
  - A conetividade de rede de gerenciamento é funcional.
  - O acesso do console ao interrutor de substituição está no lugar.
  - A imagem apropriada do sistema operacional RCF e NX-os é carregada no switch.
  - A confiugração inicial do interrutor está concluída.

Sobre esta tarefa

Este procedimento substitui o segundo switch de armazenamento Nexus 9336C-FX2 S2 com o novo switch 9336C-FX NS2. Os dois nós são node1 e node2.

Passos para concluir:

- Confirme se o interrutor a ser substituído é S2.
- Desligue os cabos do interrutor S2.
- Volte a ligar os cabos ao interrutor NS2.
- Verifique todas as configurações do dispositivo no interrutor NS2.

> Pode haver dependências entre a sintaxe de comando nas versões RCF e NX-os.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

2. Verifique o status de integridade das portas do nó de storage para garantir que haja conexão com o switch de armazenamento S1:

   ```
   storage port show -port-type ENET
   ```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage   0    enabled  offline      30
node2
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage   0    enabled  offline      30
storage::*>
```

3. Verifique se o comutador de armazenamento S1 está disponível:

   `network device-discovery show`

Mostrar exemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
--------   ----  -----------------------   ---------   ---------
node1/cdp
           e3a   S1                        Ethernet1/1 NX9336C
           e4a   node2                     e4a         AFF-A700
           e4e   node2                     e4e         AFF-A700
node1/lldp
           e3a   S1                        Ethernet1/1 -
           e4a   node2                     e4a         -
           e4e   node2                     e4e         -
node2/cdp
           e3a   S1                        Ethernet1/2 NX9336C
           e4a   node1                     e4a         AFF-A700
           e4e   node1                     e4e         AFF-A700
node2/lldp
           e3a   S1                        Ethernet1/2 -
           e4a   node1                     e4a         -
           e4e   node1                     e4e         -
storage::*>
```

4. Execute o comando show `lldp neighbors` no switch de trabalho para confirmar que você pode ver ambos os nós e todas as gavetas:

   `show lldp neighbors`

Mostrar exemplo

```
S1# show lldp neighbors
Capability codes:
   (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
   (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID        Local Intf   Hold-time    Capability    Port ID
node1            Eth1/1       121          S             e3a
node2            Eth1/2       121          S             e3a
SHFGD2008000011  Eth1/5       121          S             e0a
SHFGD2008000011  Eth1/6       120          S             e0a
SHFGD2008000022  Eth1/7       120          S             e0a
SHFGD2008000022  Eth1/8       120          S             e0a
```

5. Verifique as portas do compartimento no sistema de storage:

   `storage shelf port show -fields remote-device,remote-port`

   Mostrar exemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf   id  remote-port   remote-device
-----   --  -----------   -------------
3.20    0   Ethernet1/5   S1
3.20    1   -             -
3.20    2   Ethernet1/6   S1
3.20    3   -             -
3.30    0   Ethernet1/7   S1
3.20    1   -             -
3.30    2   Ethernet1/8   S1
3.20    3   -             -
storage::*>
```

6. Remova todos os cabos conetados ao interrutor de armazenamento S2.
7. Volte a ligar todos os cabos ao interrutor de substituição NS2.
8. Verifique novamente o status de integridade das portas do nó de storage:

   `storage port show -port-type ENET`

   Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                  Speed                      VLAN
Node              Port Type  Mode    (Gb/s) State    Status      ID
----------------- ---- ----- ------- ------ -------- --------- ----
node1
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage   0    enabled  offline     30
node2
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage   0    enabled  offline     30
storage::*>
```

9. Verifique se ambos os switches estão disponíveis:

   `network device-discovery show`

   Mostrar exemplo

```
storage::*> network device-discovery show
Node/     Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface   Platform
--------  ----  -----------------------   ---------   ---------
node1/cdp
          e3a  S1                         Ethernet1/1 NX9336C
          e4a  node2                      e4a         AFF-A700
          e4e  node2                      e4e         AFF-A700
          e7b   NS2                       Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                         Ethernet1/1 -
          e4a  node2                      e4a         -
          e4e  node2                      e4e         -
          e7b  NS2                        Ethernet1/1 -
node2/cdp
          e3a  S1                         Ethernet1/2 NX9336C
          e4a  node1                      e4a         AFF-A700
          e4e  node1                      e4e         AFF-A700
          e7b  NS2                        Ethernet1/2 NX9336C
node2/lldp
          e3a  S1                         Ethernet1/2 -
          e4a  node1                      e4a         -
          e4e  node1                      e4e         -
          e7b  NS2                        Ethernet1/2 -
storage::*>
```

10. Verifique as portas do compartimento no sistema de storage:

    `storage shelf port show -fields remote-device,remote-port`

Mostrar exemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf   id    remote-port     remote-device
-----   --    -----------     -------------
3.20    0     Ethernet1/5     S1
3.20    1     Ethernet1/5     NS2
3.20    2     Ethernet1/6     S1
3.20    3     Ethernet1/6     NS2
3.30    0     Ethernet1/7     S1
3.20    1     Ethernet1/7     NS2
3.30    2     Ethernet1/8     S1
3.20    3     Ethernet1/8     NS2
storage::*>
```

11. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

Depois de substituir seus interruptores, você"configurar monitoramento de integridade do switch" .

NVIDIA SN2100

Comece agora

Fluxo de trabalho de instalação e configuração para switches NVIDIA SN2100

O NVIDIA SN2100 é um switch Ethernet que permite alternar dados entre controladores e compartimentos de disco.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches SN2100.

1. **"Revise os requisitos de configuração"**

Revise os requisitos de configuração para o switch de armazenamento SN2100.

2. **"Revise os componentes e números de peça"**

Revise os componentes e números de peça do switch de armazenamento SN2100.

3. **"Revise a documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches SN2100 e o cluster ONTAP .

4 **"Instale o hardware"**

Instale o hardware do switch.

5 **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de rever todos os requisitos.

Requisitos de instalação

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar switches de gerenciamento adicionais, que são opcionais.

Você instala o switch NVIDIA SN2100 (X190006/X190106) no gabinete de switch dual/single NVIDIA com os suportes padrão incluídos no switch.

Para diretrizes de cabeamento, consulte"Considerações sobre cabeamento e configuração" .

Suporte a ONTAP e Linux

O switch NVIDIA SN2100 é um switch Ethernet de 10/25/40/100 GB executando o Linux Cumulus. O interrutor suporta o seguinte:

- ONTAP 9.10.1P3. O switch SN2100 serve aplicativos de cluster e armazenamento no ONTAP 9.10.1P3 em diferentes pares de switches. A partir do ONTAP 9.10.1P3, você pode usar os switches NVIDIA SN2100 para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhado.
- Cumulus Linux (CL) os versão 4,4.3. Para obter informações de compatibilidade atuais, consulte a "Switches Ethernet NVIDIA" página de informações.
- Você pode instalar o Cumulus Linux quando o switch estiver executando Cumulus Linux ou ONIE.

O que vem a seguir

"Componentes e números de peça" .

Componentes e números de peça para interrutores NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar a lista de componentes e números de peça do kit de gabinete e trilho.

Detalhes do gabinete

Você instala o switch NVIDIA SN2100 (X190006/X190106) no gabinete de switch dual/single NVIDIA com os suportes padrão incluídos no switch.

Detalhes do kit de calha

A tabela a seguir lista o número de peça e a descrição dos MSN2100 interrutores e kits de trilho:

Número de peça	Descrição
X190006-PE	Interrutor de cluster, NVIDIA SN2100, 16pt 100g, PTSX
X190006-PI	Comutador de cluster, NVIDIA SN2100, 16pt 100g, PSIN
X190106-FE-PE	Interrutor, NVIDIA SN2100, 16pt 100g, PTSX, extremidade dianteira
X190106-FE-PI	Interrutor, NVIDIA SN2100, 16pt 100g, PSIN, extremidade dianteira
X-MTEF-KIT-D	Kit de calha, interrutor duplo NVIDIA lado a lado
X-MTEF-KIT-E	Kit de calha, NVIDIA interrutor simples, profundidade curta

Consulte a documentação do NVIDIA para obter detalhes "Instalar o seu kit de comutador e calha SN2100" sobre .

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar toda a documentação recomendada.

A tabela a seguir lista a documentação disponível para os switches NVIDIA SN2100.

Título	Descrição
"*Configurar e configurar os switches NVIDIA SN2100*"	Descreve como configurar e configurar seus switches NVIDIA SN2100, incluindo a instalação do Cumulus Linux e RCFs aplicáveis.
"*Migrar de um switch de cluster Cisco para um switch de cluster NVIDIA SN2100*"	Descreve como migrar de ambientes que usam switches de cluster Cisco para ambientes que usam switches de cluster NVIDIA SN2100.
"*Migrar para um cluster comutado de dois nós com os switches de cluster NVIDIA SN2100*"	Descreve como migrar para um ambiente comutado de dois nós usando os switches de cluster NVIDIA SN2100.
"*Substitua um switch de cluster do NVIDIA SN2100*"	Descreve o procedimento para substituir um switch NVIDIA SN2100 com defeito em um cluster e fazer o download do arquivo de configuração de referência e Linux Cumulus.

Título	Descrição
"*Substitua um switch de armazenamento NVIDIA SN2100*"	Descreve o procedimento para substituir um switch de armazenamento NVIDIA SN2100 com defeito e fazer o download do arquivo de configuração de referência e Linux Cumulus.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches de armazenamento NVIDIA SN2100

Para instalar e configurar o hardware de um switch de armazenamento SN2100, siga estas etapas:

1. **"Instale o hardware"**

Instale o hardware do switch.

2. **"Analise as considerações sobre cabeamento e configuração"**

Revise os requisitos para conexões óticas, o adaptador QSA e a velocidade do switchport.

3. **"Cable as NS224 prateleiras"**

Siga os procedimentos de cabeamento se você tiver um sistema no qual os NS224 compartimentos de unidades precisam ser cabeados como storage conectado a switch (não storage com conexão direta).

Instale o hardware do switch NVIDIA SN2100

Para instalar o hardware SN2100, consulte a documentação do NVIDIA.

Passos

1. Reveja o "requisitos de configuração".
2. Siga as instruções em "Guia de instalação do interrutor NVIDIA".

O que se segue?

"Revise o cabeamento e a configuração" .

Analise as considerações sobre cabeamento e configuração

Antes de configurar o switch NVIDIA SN2100, revise as seguintes considerações.

Detalhes da porta NVIDIA

Portas de comutação	* Uso de portas*
swp1s0-3	4x10GbE breakout cluster port Nodes

swp2s0-3	4x25GbE breakout cluster port Nodes
swp3-14	Nós de porta de cluster 40/100GbE
swp15-16	100GbE portas ISL (Inter-Switch Link)

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Atrasos de ligação com ligações óticas

Se você estiver enfrentando atrasos de link-up de mais de cinco segundos, o Cumulus Linux 5,4 e posterior inclui suporte para link-up rápido. Você pode configurar os links usando o `nv set` comando da seguinte forma:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Mostrar exemplo

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Suporte para conexões de cobre

As seguintes alterações de configuração são necessárias para corrigir esse problema.

Cumulus Linux 4.4.3

1. Identifique o nome de cada interface usando cabos de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Adicione as duas linhas a seguir ao `/etc/cumulus/switchd.conf` arquivo para cada porta (swp<n>) que esteja usando cabos de cobre 40GbE/100GbE:

   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   Por exemplo:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Reinicie `switchd` o serviço:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirme se as portas estão ativas:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
```

Cumulus Linux 5.x

1. Identifique o nome de cada interface usando cabos de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Configure os links usando o `nv set` comando da seguinte forma:

   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Recarregue o `switchd` serviço

     Por exemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Confirme se as portas estão ativas:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode        LLDP                Summary
-----  --------- ----  -----  ----------  ------------------  --------
UP     swp3      100G  9216   Trunk/L2                        Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                        Master:
bridge(UP)
```

Consulte o artigo da base de dados de Conhecimento "O switch SN2100 não consegue se conetar usando cabos de cobre 40/100GbE" para obter mais detalhes.

No Cumulus Linux 4,4.2, as conexões de cobre não são suportadas em switches SN2100 com X1151A portas NIC, X1146A NIC ou 100GbE integradas. Por exemplo:

- AFF A800 nas portas e0a e e0b
- AFF A320 nas portas e0g e e0h

Adaptador QSA

Quando um adaptador QSA é usado para se conetar às portas de cluster 10GbE/25GbE em uma plataforma, o link pode não aparecer.

Para resolver esse problema, faça o seguinte:

- Para 10GbE, defina manualmente a velocidade do link swp1s0-3 para 10000 e defina a negociação automática como desativada.
- Para 25GbE, defina manualmente a velocidade do link swp2s0-3 para 25000 e defina a negociação automática como desativada.

> Ao usar adaptadores QSA 10GbE/25GbE, insira-os em portas 40GbE/100GbE não-breakout (swp3-swp14). Não insira o adaptador QSA em uma porta configurada para breakout.

Defina a velocidade da interface nas portas de arranque

Dependendo do transcetor na porta do switch, talvez seja necessário definir a velocidade na interface do switch para uma velocidade fixa. Se estiver usando portas multiconexões 10GbE e 25GbE, verifique se a negociação automática está desligada e defina a velocidade da interface no switch.

Cumulus Linux 4.4.3

Por exemplo:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces     2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000  <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
     alias 10G Intra-Cluster Node
-    link-autoneg off
+    link-autoneg on
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp2s0
iface swp2s0
     alias 25G Intra-Cluster Node
     link-autoneg off
     link-speed 25000 <---- port speed set
```

Verifique a interface e o status da porta para verificar se as configurações são aplicadas:

```
cumulus@cumulus:mgmt:~$ net show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Cumulus Linux 5.x

Por exemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate        off                     off
off
  duplex                full                    full
full
  speed                 10G                     10G
10G
  fec                   auto                    auto
auto
  mtu                   9216                    9216
9216
[breakout]

  state                 up                      up
up
```

Verifique a interface e o status da porta para verificar se as configurações são aplicadas:

```
cumulus@cumulus:mgmt:~$ nv show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

O que se segue?

"Cabo NS224 prateleiras como storage conetado a switch".

Cabo NS224 prateleiras como storage conetado a switch

Se você tiver um sistema no qual os NS224 compartimentos de unidades precisem ser cabeados como storage conectado ao switch (não storage com conexão direta), use as informações fornecidas aqui.

- Cabos NS224 shelves de unidade através de switches de armazenamento:

  "Informações sobre cabeamento de compartimentos de unidades NS224 conectados a switch"

- Instale os switches de armazenamento:

  "Documentação do comutador AFF e FAS"

- Confirme o hardware suportado, como switches de armazenamento e cabos, para o modelo da sua plataforma:

  "NetApp Hardware Universe"

Configure o software

Fluxo de trabalho de instalação de software para switches de storage NVIDIA SN2100

Para instalar e configurar o software para um switch NVIDIA SN2100, siga estas etapas:

1. **"Configure o interrutor"**

   Configurar o switch NVIDIA SN2100.

2. **"Instale o Cumulus Linux no modo Cumulus"**

   Você pode instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver executando o Cumulus Linux.

3. **"Instale o Cumulus Linux no modo ONIE"**

   Como alternativa, você pode instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver executando o Cumulus Linux no modo ONIE.

4. **"Instale o script RCF (Reference Configuration File)"**

   Existem dois scripts RCF disponíveis para aplicativos de agrupamento e armazenamento. O procedimento para cada um é o mesmo.

5. **"Instale o arquivo CSHM"**

   Você pode instalar o arquivo de configuração aplicável para o monitoramento de integridade do switch Ethernet dos switches de cluster NVIDIA.

6. **"Redefinir o switch para os padrões de fábrica"**

   Apague as configurações do switch de armazenamento SN2100.

Configure o switch NVIDIA SN2100

Para configurar o switch SN2100, consulte a documentação do NVIDIA.

Passos

1. Reveja o "requisitos de configuração".
2. Siga as instruções em "Apresentação do sistema NVIDIA.".

O que se segue?

"Instale o Cumulus Linux no modo Cumulus"ou"Instale o Cumulus Linux no modo ONIE" .

Instale o Cumulus Linux no modo Cumulus

Siga este procedimento para instalar o SO Cumulus Linux (CL) quando o switch estiver em execução no modo Cumulus.

O SO Cumulus Linux (CL) pode ser instalado quando o switch está executando o Cumulus Linux ou ONIE ("Instale no modo ONIE"consulte).

Antes de começar

Certifique-se de que o seguinte esteja disponível:

- Conhecimento do Linux de nível intermediário.
- Familiaridade com edição de texto básica, permissões de arquivo UNIX e monitoramento de processos. Uma variedade de editores de texto são pré-instalados, `vi` incluindo e `nano`.
- Acesso a um shell Linux ou UNIX. Se você estiver executando o Windows, use um ambiente Linux como sua ferramenta de linha de comando para interagir com o Cumulus Linux.
- O requisito de taxa de transmissão deve ser definido como 115200 no switch do console serial para acesso ao console do switch NVIDIA SN2100, como segue:
  - 115200 baud
  - 8 bits de dados
  - 1 bit de paragem
  - paridade: nenhuma
  - controle de fluxo: nenhum

Sobre esta tarefa

Tenha em atenção o seguinte:

Cada vez que o Cumulus Linux é instalado, toda a estrutura do sistema de arquivos é apagada e reconstruída.

A senha padrão para a conta de usuário do Cumulus é **Cumulus**. A primeira vez que você fizer login no Cumulus Linux, você deve alterar essa senha padrão. Certifique-se de atualizar quaisquer scripts de automação antes de instalar uma nova imagem. O Cumulus Linux fornece opções de linha de comando para alterar a senha padrão automaticamente durante o processo de instalação.

Exemplo 6. Passos

Cumulus Linux 4.4.3

1. Inicie sessão no interrutor.

   O login pela primeira vez no switch requer nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo` o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

   Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina a data, a hora, o fuso horário e o servidor NTP no switch.
   a. Verifique o fuso horário atual:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Atualizar para o novo fuso horário:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

d. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

i. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Instale o Cumulus Linux 4,4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 4,4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

Cumulus Linux 5.4.0

1. Inicie sessão no interrutor.

   O login pela primeira vez no switch requer nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo`

o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

> Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

> Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina o fuso horário, a data, a hora e o servidor NTP no switch.
   a. Defina o fuso horário:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

   c. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

   d. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Veja o artigo da Base de Conhecimento "A configuração do servidor NTP não está funcionando com os switches NVIDIA SN2100" para mais detalhes.

g. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale o Cumulus Linux 5,4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 5,4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 13:37:36     system uptime
timezone            Etc/UTC              system time zone
```

11. Verifique se os nós têm uma conexão com cada switch:

```
cumulus@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   Mgmt        mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

12. Crie um novo usuário e adicione esse usuário ao `sudo` grupo. Este usuário só se torna efetivo após a sessão console/SSH ser reiniciada.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Adicione grupos de usuários adicionais para que o usuário admin acesse `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user 'admin' to group 'nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

Cumulus Linux 5.11.0

1. Inicie sessão no interrutor.

   Quando você faz login no switch pela primeira vez, ele requer o nome de usuário/senha do **Cumulus**/**Cumulus** com `sudo` o Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Verifique a versão Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Configure o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão. O novo nome de host só se torna efetivo após reiniciar a sessão console/SSH.

   Um switch Cumulus Linux fornece pelo menos uma porta de gerenciamento Ethernet dedicada `eth0` chamada . Esta interface é especificamente para uso de gerenciamento fora da banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.

   Não use um sublinhado (_), apóstrofo (') ou carateres não-ASCII no nome do host.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica os `/etc/hostname` ficheiros e `/etc/hosts`.

4. Confirme se o nome do host, o endereço IP, a máscara de sub-rede e o gateway padrão foram atualizados.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Defina o fuso horário, a data, a hora e o servidor NTP no switch.
   a. Defina o fuso horário:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verifique o fuso horário atual:

```
cumulus@switch:~$ date +%Z
```

   c. Para definir o fuso horário usando o assistente guiado, execute o seguinte comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Defina o relógio do software de acordo com o fuso horário configurado:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Defina o valor atual do relógio do software para o relógio do hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Adicione um servidor NTP, se necessário:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Veja o artigo da Base de Conhecimento "A configuração do servidor NTP não está funcionando com os switches NVIDIA SN2100" para mais detalhes.

g. Verifique se `ntpd` está em execução no sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique a interface de origem NTP. Por padrão, a interface de origem que o NTP usa é `eth0`. Você pode configurar uma interface de origem NTP diferente da seguinte forma:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale o Cumulus Linux 5,11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

O instalador inicia a transferência. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação é iniciada automaticamente e as seguintes opções de tela GRUB são exibidas. **Não** faça nenhuma seleção.
   - Cumulus-Linux GNU/Linux
   - ONIE: Instale os
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repita os passos 1 a 4 para iniciar sessão.
10. Verifique se a versão Cumulus Linux é 5,11.0:

    `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied                 description
------------------- ----------------------- --------------------
build               Cumulus Linux 5.11.0
uptime              153 days, 2:44:16
hostname            cumulus                 cumulus
product-name        Cumulus Linux
product-release     5.11.0
platform            x86_64-mlnx_x86-r0
system-memory       2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory         0 Bytes used / 0 Bytes free / 0 Bytes total
health-status       not OK
date-time           2025-04-23 09:55:24
status              N/A
timezone            Etc/UTC
maintenance
  mode              disabled
  ports             enabled
version
  kernel            6.1.0-cl-1-amd64
  build-date        Thu Nov 14 13:06:38 UTC 2024
  image             5.11.0
  onie              2019.11-5.2.0020-115200
```

11. Verifique se cada nó tem uma conexão com cada switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   eth   mgmt-sw1
Eth110/1/14
swp2s1     25G    Trunk/L2    node1
e0a
swp1s1     10G    swp   sw2
e0a
swp9       100G   swp   sw3
e4a
swp10      100G   swp   sw4
e4a
swp15      100G   swp   sw5
swp15
swp16      100G   swp   sw6
swp16
```

Consulte "Contas de usuário do NVIDIA" para obter mais informações.

O que se segue?

"Instale ou atualize o script RCF" .

Instale o Cumulus Linux no modo ONIE

Siga este procedimento para instalar o SO Cumulus Linux (CL) quando o switch estiver em execução no modo ONIE.

> O SO Cumulus Linux (CL) pode ser instalado quando o switch está executando o Cumulus Linux ou ONIE ("Instale no modo Cumulus"consulte).

Sobre esta tarefa

Você pode instalar o Cumulus Linux usando o Open Network Install Environment (ONIE) que permite a descoberta automática de uma imagem do instalador de rede. Isso facilita o modelo de sistema de proteção de switches com uma escolha de sistema operacional, como o Cumulus Linux. A maneira mais fácil de instalar o Cumulus Linux com ONIE é com descoberta HTTP local.

> Se o seu host estiver habilitado para IPv6, verifique se ele está executando um servidor da Web. Se o seu host estiver habilitado para IPv4, verifique se ele está executando o DHCP além de um servidor da Web.

Este procedimento demonstra como atualizar o Cumulus Linux após o administrador ter inicializado no ONIE.

Passos

1. Baixe o arquivo de instalação Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo `onie-installer`.
2. Conete o host à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interrutor. O switch faz o download do instalador de imagem ONIE e inicializa. Após a conclusão da instalação, o prompt de login do Cumulus Linux aparece na janela do terminal.

   Cada vez que o Cumulus Linux é instalado, toda a estrutura do sistema de arquivos é apagada e reconstruída.

4. Reinicie o switch SN2100:

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

5. Pressione a tecla **ESC** na tela GNU GRUB para interromper o processo de inicialização normal, selecione **ONIE** e pressione **Enter**.
6. Na próxima tela exibida, selecione **ONIE: Install os**.
7. O processo de descoberta do instalador ONIE é executado procurando a instalação automática. Pressione **Enter** para interromper temporariamente o processo.
8. Quando o processo de descoberta for interrompido:

   ```
   ONIE:/ # onie-stop
   discover: installer mode detected.
   Stopping: discover...start-stop-daemon: warning: killing process 427:
   No such process done.
   ```

9. Se o serviço DHCP estiver em execução na rede, verifique se o endereço IP, a máscara de sub-rede e o gateway padrão estão corretamente atribuídos:

   ```
   ifconfig eth0
   ```

Mostrar exemplo

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.233.204.1    0.0.0.0         UG    0      0
0   eth0
10.233.204.0    *               255.255.254.0   U     0      0
0   eth0
```

10. Se o esquema de endereçamento IP for definido manualmente, faça o seguinte:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Repita o passo 9 para verificar se as informações estáticas foram introduzidas corretamente.
12. Instale o Cumulus Linux:

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-
4.4.3-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

13. Depois de concluída a instalação, inicie sessão no interrutor:

Mostrar exemplo

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

14. Verifique a versão Cumulus Linux:

```
net show version
```

Mostrar exemplo

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3”
```

O que se segue?

"Instale ou atualize o script RCF" .

Instale ou atualize o script RCF

Siga este procedimento para instalar ou atualizar o script RCF.

Antes de começar

Antes de instalar ou atualizar o script RCF, certifique-se de que o seguinte está disponível no switch:

- Cumulus Linux 4.4.3 está instalado.
- Endereço IP, máscara de sub-rede e gateway padrão definido via DHCP ou configurado manualmente.

Versões de script RCF atuais

Existem dois scripts RCF disponíveis para aplicativos de agrupamento e armazenamento. O procedimento para cada um é o mesmo.

- Clustering: **MSN2100-RCF-v1.*x*-Cluster**
- Armazenamento: **MSN2100-RCF-v1.*x*-Storage**

> O procedimento de exemplo a seguir mostra como baixar e aplicar o script RCF para switches de cluster.

> Exemplo de saída de comando usa o endereço IP de gerenciamento de switch 10.233.204.71, máscara de rede 255.255.254.0 e gateway padrão 10.233.204.1.

Passos

1. Apresentar as interfaces disponíveis no interrutor SN2100:

```
net show interface all
```

Mostrar exemplo

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name   Spd  MTU    Mode         LLDP                 Summary
-----  -----  ---  -----  -----------  -------------------
--------------
...
...
ADMDN  swp1   N/A  9216   NotConfigured
ADMDN  swp2   N/A  9216   NotConfigured
ADMDN  swp3   N/A  9216   NotConfigured
ADMDN  swp4   N/A  9216   NotConfigured
ADMDN  swp5   N/A  9216   NotConfigured
ADMDN  swp6   N/A  9216   NotConfigured
ADMDN  swp7   N/A  9216   NotConfigure
ADMDN  swp8   N/A  9216   NotConfigured
ADMDN  swp9   N/A  9216   NotConfigured
ADMDN  swp10  N/A  9216   NotConfigured
ADMDN  swp11  N/A  9216   NotConfigured
ADMDN  swp12  N/A  9216   NotConfigured
ADMDN  swp13  N/A  9216   NotConfigured
ADMDN  swp14  N/A  9216   NotConfigured
ADMDN  swp15  N/A  9216   NotConfigured
ADMDN  swp16  N/A  9216   NotConfigured
```

2. Copie o script Python do RCF para o switch:

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster                 100% 8607   111.2KB/s
00:00
```

3. Aplique o script Python RCF **MSN2100-RCF-v1,8-Cluster**:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

O script RCF completa as etapas listadas acima.

> Para quaisquer problemas de script Python do RCF que não possam ser corrigidos, entre em Contato "Suporte à NetApp" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
5. Verifique a configuração após a reinicialização:

   ```
   net show interface all
   ```

Mostrar exemplo

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP                Summary
-----  --------- ----  -----  ---------- ------------------ --------
...
...
DN     swp1s0    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s1    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s2    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp1s3    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp2s0    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp2s1    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp2s2    N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp2s3    N/A   9216   Trunk/L2                       Master:
bridge(UP)
UP     swp3      100G  9216   Trunk/L2                       Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                       Master:
bridge(UP)
DN     swp5      N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp6      N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp7      N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp8      N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp9      N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp10     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp11     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp12     N/A   9216   Trunk/L2                       Master:
bridge(UP)
DN     swp13     N/A   9216   Trunk/L2                       Master:
bridge(UP)
```

```
DN     swp14     N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp15     N/A   9216   BondMember                  Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                  Master:
bond_15_16(UP)
...
...

cumulus@cumulus:mgmt:~$ net show roce config
RoCE mode..... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
  Mode..... ECN
  Min Threshold.. 150 KB
  Max Threshold.. 1500 KB
PFC:
  Status..... enabled
  Enabled SPs.... 2 5
  Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9

DSCP                    802.1p  switch-priority
----------------------  ------  ---------------
0 1 2 3 4 5 6 7              0                0
8 9 10 11 12 13 14 15        1                1
16 17 18 19 20 21 22 23      2                2
24 25 26 27 28 29 30 31      3                3
32 33 34 35 36 37 38 39      4                4
40 41 42 43 44 45 46 47      5                5
48 49 50 51 52 53 54 55      6                6
56 57 58 59 60 61 62 63      7                7

switch-priority  TC  ETS
---------------  --  --------
0 1 3 4 6 7       0  DWRR 28%
2                 2  DWRR 28%
5                 5  DWRR 43%
```

6. Verifique as informações do transcetor na interface:

```
net show interface pluggables
```

Mostrar exemplo

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor SN
    Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp3       0x11 (QSFP28)  Amphenol     112-00574
APF20379253516  B0
swp4       0x11 (QSFP28)  AVAGO        332-00440        AF1815GU05Z
    A0
swp15      0x11 (QSFP28)  Amphenol     112-00573
APF21109348001  B0
swp16      0x11 (QSFP28)  Amphenol     112-00573
APF21109347895  B0
```

7. Verifique se os nós têm uma conexão com cada switch:

   `net show lldp`

Mostrar exemplo

```
cumulus@cumulus:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost              RemotePort
---------  -----  ----------  ----------------------  -----------
swp3       100G   Trunk/L2    sw1                     e3a
swp4       100G   Trunk/L2    sw2                     e3b
swp15      100G   BondMember  sw13                    swp15
swp16      100G   BondMember  sw14                    swp16
```

8. Verifique a integridade das portas de cluster no cluster.

   a. Verifique se as portas e0d estão ativas e íntegras em todos os nós do cluster:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

a. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch SW2, uma vez que LIFs não são homed em e0d).

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

O que se segue?

"Instale o arquivo CSHM".

Instale o arquivo de configuração do Monitor de integridade do comutador Ethernet

Siga este procedimento para instalar o arquivo de configuração aplicável para o monitoramento de integridade do switch Ethernet dos switches do cluster NVIDIA. Os modelos suportados são:

- MSN2100-CB2FC
- MSN2100-CB2RC
- X190006-PE
- X190006-PI

Este procedimento de instalação aplica-se ao ONTAP 9.10,1 e posterior.

Antes de começar

- Verifique se é necessário fazer o download do arquivo de configuração executando `system switch ethernet show` e verificando se **OTHER** é mostrado para o seu modelo.

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

- Certifique-se de que o cluster do ONTAP está ativo e em execução.
- Ative o SSH 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 conetados.

  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 cluster-switch configure-health-monitor -node *
-package-url http://192.168.2.20/usr/download/[filename.zip]
```

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 show` no sistema ONTAP e certifique-se de que os switches de cluster são descobertos com o campo monitorado definido como **True** e o campo de número de série não mostrando **desconhecido**.

```
cluster1::> system switch ethernet show
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Redefinir o switch de armazenamento SN2100 para os padrões de fábrica

Para redefinir o switch de armazenamento SN2100 para os padrões de fábrica:

- Para o Cumulus Linux 5.10 e anteriores, aplique a imagem Cumulus.
- Para Cumulus Linux 5.11 e posterior, você usa o `nv action reset system factory-default` comando.

Sobre esta tarefa

- Você deve estar conetado ao switch usando o console serial.
- Você precisa ter a senha de root para ter acesso sudo aos comandos.

Para obter mais informações sobre a instalação do Cumulus Linux, consulte"Fluxo de trabalho de instalação de software para switches NVIDIA SN2100" .

Exemplo 7. Passos

Cumulus Linux 5.10 e anteriores

1. No console Cumulus, baixe e coloque na fila a instalação do software do switch com o comando `onie-install -a -i` seguido pelo caminho do arquivo para o software do switch, por exemplo:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. O instalador inicia o download. Digite **y** quando solicitado para confirmar a instalação quando a imagem for baixada e verificada.
3. Reinicie o switch para instalar o novo software.

   `sudo reboot`

```
cumulus@sw1:mgmt:~$ sudo reboot
```

> O switch é reinicializado e entra na instalação do software do switch, o que leva algum tempo. Quando a instalação estiver concluída, o switch será reinicializado e permanecerá no estado `log-in` incitar.

Cumulus Linux 5.11 e posterior

1. Para redefinir o switch para os padrões de fábrica e remover todas as configurações, arquivos de sistema e arquivos de log, execute:

   `nv action reset system factory-default`

   Por exemplo:

```
cumulus@switch:~$ nv action reset system factory-default

This operation will reset the system configuration, delete the log
files and reboot the switch.
Type [y] continue.
Type [n] to abort.
Do you want to continue? [y/n] y
```

Veja a NVIDIA "Redefinição de fábrica" documentação para mais detalhes.

Migrar switches

Migre de um switch de storage Cisco para um switch de storage NVIDIA SN2100

É possível migrar switches Cisco mais antigos para um cluster ONTAP para switches de storage NVIDIA SN2100. Este é um procedimento sem interrupções.

Rever os requisitos

Os seguintes switches de armazenamento são suportados:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Consulte o "Hardware Universe" para obter detalhes completos sobre as portas suportadas e respetivas configurações.

Antes de começar

Certifique-se de ter o seguinte:

- O cluster existente está corretamente configurado e funcionando.
- Todas as portas de storage estão no estado operacional para garantir operações ininterruptas.
- Os switches de armazenamento NVIDIA SN2100 são configurados e operando sob a versão adequada do Cumulus Linux instalado com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede de armazenamento existente tem o seguinte:
  - Um cluster NetApp redundante e totalmente funcional usando ambos os switches Cisco mais antigos.
  - Conetividade de gerenciamento e acesso ao console aos switches Cisco mais antigos e aos novos switches.
  - Todas as LIFs de cluster no estado up com os LIfs de cluster estão em suas portas iniciais.
  - Portas ISL ativadas e cabeadas entre os switches Cisco mais antigos e entre os novos switches.
- Consulte o "Hardware Universe" para obter detalhes completos sobre as portas suportadas e respetivas configurações.
- Algumas das portas são configuradas nos switches NVIDIA SN2100 para serem executadas a 100 GbE.
- Você planejou, migrou e documentou a conectividade de 100 GbE de nós para os switches de storage NVIDIA SN2100.

Migrar os switches

Sobre os exemplos

Neste procedimento, os switches de armazenamento Cisco Nexus 9336C-FX2 são usados, por exemplo, comandos e saídas.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de armazenamento Cisco Nexus 9336C-FX2 existentes são *S1* e *S2*.
- Os novos switches de armazenamento NVIDIA SN2100 são *SW1* e *SW2*.
- Os nós são *node1* e *node2*.
- Os LIFs de cluster são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.

- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de rede usadas neste procedimento são *E5A* e *e5b*.
- As portas breakout tomam o formato: Swp1s0-3. Por exemplo, quatro portas breakout no swp1 são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.
- O interrutor S2 é substituído primeiro pelo interrutor SW2 e, em seguida, o interrutor S1 é substituído pelo interrutor SW1.
  - O cabeamento entre os nós e o S2 é desconetado do S2 e reconetado ao SW2.
  - O cabeamento entre os nós e o S1 é desconetado do S1 e reconetado ao SW1.

Passo 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde *x* é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   `set -privilege advanced`

   É apresentado o aviso avançado (*>).

3. Determine o status administrativo ou operacional de cada interface de storage:

   Cada porta deve exibir habilitado para `Status`.

Etapa 2: Configurar cabos e portas

1. Exibir os atributos da porta de rede:

   `storage port show`

Mostrar exemplo

```
cluster1::*> storage port show
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

2. Verifique se as portas de storage em cada nó estão conetadas aos switches de storage existentes da seguinte maneira (da perspetiva dos nós) usando o comando:

   `network device-discovery show -protocol lldp`

   Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/1           -
node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/2           -
```

3. No switch S1 e S2, certifique-se de que as portas de armazenamento e os switches estão conetados da seguinte maneira (da perspetiva dos switches) usando o comando:

   `show lldp neighbors`

Mostrar exemplo

```
S1# show lldp neighbors

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,
                  (W) WLAN Access Point, (P) Repeater, (S) Station
(O) Other

Device-ID             Local Intf     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e0c
node2                 Eth1/2         121         S
e0c
SHFGD1947000186       Eth1/10        120         S
  e0a
SHFGD1947000186       Eth1/11        120         S
  e0a
SHFGB2017000269       Eth1/12        120         S
  e0a
SHFGB2017000269       Eth1/13        120         S
  e0a

S2# show lldp neighbors

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,
                  (W) WLAN Access Point, (P) Repeater, (S) Station
(O) Other

Device-ID             Local Intf     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e5b
node2                 Eth1/2         121         S
e5b
SHFGD1947000186       Eth1/10        120         S
 e0b
SHFGD1947000186       Eth1/11        120         S
 e0b
SHFGB2017000269       Eth1/12        120         S
 e0b
SHFGB2017000269       Eth1/13        120         S
 e0b
```

4. No switch SW2, encerre as portas conectadas às portas de storage e aos nós das gavetas de disco.

Mostrar exemplo

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Mova as portas de storage de nós da controladora e das gavetas de disco do switch antigo S2 para o novo switch SW2, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
6. No switch SW2, abra as portas conectadas às portas de storage dos nós e das gavetas de disco.

Mostrar exemplo

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Verifique se as portas de storage em cada nó agora estão conetadas aos switches da seguinte maneira, da perspetiva dos nós:

```
network device-discovery show -protocol lldp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1           -

node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp2           -
```

8. Verifique os atributos da porta de rede:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
                                  Speed                      VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

9. No switch SW2, verifique se todas as portas de storage de nós estão ativas:

   `net show interface`

Mostrar exemplo

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

10. No switch SW1, encerre as portas conectadas às portas de storage dos nós e das gavetas de disco.

Mostrar exemplo

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Mova as portas de storage de nós da controladora e das gavetas de disco do switch antigo S1 para o novo switch SW1, usando o cabeamento apropriado suportado pelo NVIDIA SN2100.
12. No switch SW1, abra as portas conectadas às portas de storage dos nós e das gavetas de disco.

Mostrar exemplo

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Verifique se as portas de storage em cada nó agora estão conetadas aos switches da seguinte maneira, da perspetiva dos nós:

    `network device-discovery show -protocol lldp`

    Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    sw1 (b8:ce:f6:19:1b:96)   swp1            -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1            -

node2      /lldp
            e0c    sw1  (b8:ce:f6:19:1b:96)  swp2            -
            e5b    sw2  (b8:ce:f6:19:1a:7e)  swp2            -
```

Etapa 3: Verifique a configuração

1. Verifique a configuração final:

   `storage port show`

   Cada porta deve ser exibida habilitada para `State` e ativada para `Status`.

Mostrar exemplo

```
cluster1::*> storage port show
                                  Speed                      VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

2. No switch SW2, verifique se todas as portas de storage de nós estão ativas:

   `net show interface`

Mostrar exemplo

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

3. Verifique se ambos os nós têm uma conexão com cada switch:

   `net show lldp`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cumulus@sw1:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost              RemotePort
---------  -----  --------  --------------------  -----------
...
swp1       100G   Trunk/L2  node1                 e0c
swp2       100G   Trunk/L2  node2                 e0c
swp3       100G   Trunk/L2  SHFFG1826000112       e0a
swp4       100G   Trunk/L2  SHFFG1826000112       e0a
swp5       100G   Trunk/L2  SHFFG1826000102       e0a
swp6       100G   Trunk/L2  SHFFG1826000102       e0a

cumulus@sw2:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost              RemotePort
---------  -----  --------  --------------------  -----------
...
swp1       100G   Trunk/L2  node1                 e5b
swp2       100G   Trunk/L2  node2                 e5b
swp3       100G   Trunk/L2  SHFFG1826000112       e0b
swp4       100G   Trunk/L2  SHFFG1826000112       e0b
swp5       100G   Trunk/L2  SHFFG1826000102       e0b
swp6       100G   Trunk/L2  SHFFG1826000102       e0b
```

4. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

5. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua um interrutor de armazenamento NVIDIA SN2100

Você pode substituir um switch de armazenamento NVIDIA SN2100 com defeito. Este é um procedimento sem interrupções.

Antes de começar

Antes de instalar o software Cumulus e os RCFs em um switch de armazenamento NVIDIA SN2100, certifique-se de que:

- Seu sistema pode suportar switches de armazenamento NVIDIA SN2100.
- Você baixou os RCFs aplicáveis.

O "Hardware Universe" fornece detalhes completos das portas suportadas e respetivas configurações.

A configuração de rede existente deve ter as seguintes caraterísticas:

- Conclua todas as etapas de solução de problemas para confirmar que você precisa substituir seu switch.
- Garanta que a conectividade de gerenciamento exista em ambos os switches.

> Certifique-se de que todas as etapas de solução de problemas foram concluídas para confirmar que o switch precisa ser substituído.

O interrutor NVIDIA SN2100 de substituição deve ter as seguintes caraterísticas:

- A conetividade de rede de gerenciamento é funcional.
- Você pode acessar o interruptor de substituição usando o console.
- A imagem apropriada do sistema operacional RCF e Cumulus é carregada no switch.
- A personalização inicial do switch está concluída.

Resumo do procedimento

Este procedimento substitui o segundo interrutor de armazenamento NVIDIA SN2100 SW2 pelo novo interrutor NVIDIA SN2100 nsw2. Os dois nós são node1 e node2.

Passos para concluir:

- Confirme se o interrutor a ser substituído é SW2.
- Desligue os cabos do interrutor SW2.
- Volte a ligar os cabos ao interrutor nsw2.
- Verifique todas as configurações do dispositivo no interrutor nsw2.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

3. Verifique o status de integridade das portas do nó de armazenamento para confirmar a conexão com o switch de armazenamento S1:

   ```
   storage port show -port-type ENET
   ```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage 100    enabled  online       30
node2
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage 100    enabled  online       30
cluster1::*>
```

4. Verifique se o comutador de armazenamento SW1 está disponível:

   `network device-discovery show -protocol lldp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

5. Execute o `net show interface` comando no switch de trabalho para confirmar que você pode ver ambos os nós e todas as gavetas:

   `net show interface`

Mostrar exemplo

```
cumulus@sw1:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e3a)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e3a)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

6. Verifique as portas do compartimento no sistema de storage:

   `storage shelf port show -fields remote-device, remote-port`

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id  remote-port   remote-device
-----   --  -----------   -------------
3.20    0   swp3          sw1
3.20    1   -             -
3.20    2   swp4          sw1
3.20    3   -             -
3.30    0   swp5          sw1
3.20    1   -             -
3.30    2   swp6          sw1
3.20    3   -             -
cluster1::*>
```

7. Remova todos os cabos conetados ao interrutor de armazenamento SW2.
8. Volte a ligar todos os cabos ao interrutor de substituição nsw2.
9. Verifique novamente o status de integridade das portas do nó de storage:

   `storage port show -port-type ENET`

   Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
                                    Speed                      VLAN
Node              Port Type  Mode    (Gb/s) State    Status      ID
----------------- ---- ----- ------- ------ -------- --------- ----
node1
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage 100    enabled  online      30
node2
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage 100    enabled  online      30
cluster1::*>
```

10. Verifique se ambos os switches estão disponíveis:

    `net device-discovery show -protocol lldp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

11. Verifique as portas do compartimento no sistema de storage:

    `storage shelf port show -fields remote-device, remote-port`

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id    remote-port     remote-device
-----   --    -----------     -------------
3.20    0     swp3            sw1
3.20    1     swp3            nsw2
3.20    2     swp4            sw1
3.20    3     swp4            nsw2
3.30    0     swp5            sw1
3.20    1     swp5            nsw2
3.30    2     swp6            sw1
3.20    3     swp6            nsw2
cluster1::*>
```

12. Altere o nível de privilégio de volta para admin:

    ```
    set -privilege admin
    ```

13. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

    ```
    system node autosupport invoke -node * -type all -message MAINT=END
    ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Switches compartilhados

Cisco Nexus 9336C-FX2

Comece agora

Fluxo de trabalho de instalação e configuração para switches compartilhados Cisco Nexus 9336C-FX2

O switch compartilhado Cisco Nexus 9336C-FX2 faz parte da plataforma Cisco Nexus 9000 e pode ser instalado em um gabinete de sistema NetApp. Os switches compartilhados permitem combinar a funcionalidade de cluster e armazenamento em uma configuração de switch compartilhado, suportando o uso de arquivos de configuração de referência de cluster e armazenamento compartilhados.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches Cisco 9336C-FX2.

1. **"Revise os requisitos de configuração"**

Revise os requisitos de configuração para o switch compartilhado 9336C-FX2.

2. **"Revise os componentes e números de peça"**

Revise os componentes e números de peça do switch compartilhado 9336C-FX2.

3. **"Revise a documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 9336C-FX2 e o cluster ONTAP .

Requisitos de configuração para switches compartilhados Cisco Nexus 9336C-FX2

Para a instalação e manutenção do switch Cisco Nexus 9336C-FX2, certifique-se de rever os requisitos de configuração e rede.

Suporte à ONTAP

A partir do ONTAP 9.9,1, você pode usar os switches Cisco Nexus 9336C-FX2 para combinar a funcionalidade de armazenamento e cluster em uma configuração de switch compartilhado.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

Requisitos de configuração

Para a configuração, você precisa do número e tipo apropriados de cabos e conetores de cabo para seus switches.

Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de

rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para o tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700s, a interface e0M utiliza uma porta Ethernet dedicada.
- Consulte a "Hardware Universe" para obter as informações mais recentes.

Para obter mais informações sobre a configuração inicial do switch, consulte o seguinte guia: "Guia de instalação e atualização do Cisco Nexus 9336C-FX2".

O que vem a seguir

"Componentes e números de peça" .

Componentes e números de peça para switches compartilhados Cisco Nexus 9336C-FX2

Para instalação e manutenção do switch Cisco Nexus 9336C-FX2, certifique-se de rever a lista de componentes e números de peça.

A tabela a seguir lista o número de peça e a descrição do interrutor 9336C-FX2, ventiladores e fontes de alimentação:

Número de peça	Descrição
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190002	Kit de acessórios X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336CA AC 1100W PSU - fluxo de ar do escape lateral da porta
X-NXA-PAC-1100W-PI2	N9K-9336CA AC 1100W PSU - fluxo de ar de entrada lateral da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, fluxo de ar do escape lateral da porta
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, fluxo de ar de admissão do lado da porta

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2

Para a instalação e manutenção do switch Cisco Nexus 9336C-FX2, verifique a documentação específica do switch e do controlador para configurar os switches Cisco 9336-FX2 e o cluster ONTAP.

Para configurar os switches compartilhados do Cisco Nexus 9336C-FX2, consulte a "Suporte para switches Cisco Nexus 9000 Series" página.

Título do documento	Descrição
"Guia de instalação de hardware do Nexus 9000 Series"	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
"Guias de configuração do software de switch Cisco Nexus 9000 Series" (Escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
"Guia de atualização e downgrade de software Cisco Nexus 9000 Series NX-os" (Escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
"Índice mestre de referência de comando Cisco Nexus 9000 Series NX-os"	Fornece links para as várias referências de comando fornecidas pelo Cisco.
"Referência de MIBs Cisco Nexus 9000"	Descreve os arquivos MIB (Management Information base) para os switches Nexus 9000.
"Referência de mensagem do sistema Nexus 9000 Series NX-os"	Descreve as mensagens do sistema para os switches da série Cisco Nexus 9000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
"Notas de lançamento do Cisco 9000 NX-os" (Escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 9000 Series.
"Conformidade regulamentar e informações de segurança para a série Cisco Nexus 9000"	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 9000.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches compartilhados Cisco Nexus 9336C-FX2

Para instalar e configurar o hardware de um switch compartilhado 9336C-FX2, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2 **"Instale o interrutor"**

Instale o switch 9336C-FX2.

3 **"Instale o interrutor em um gabinete NetApp"**

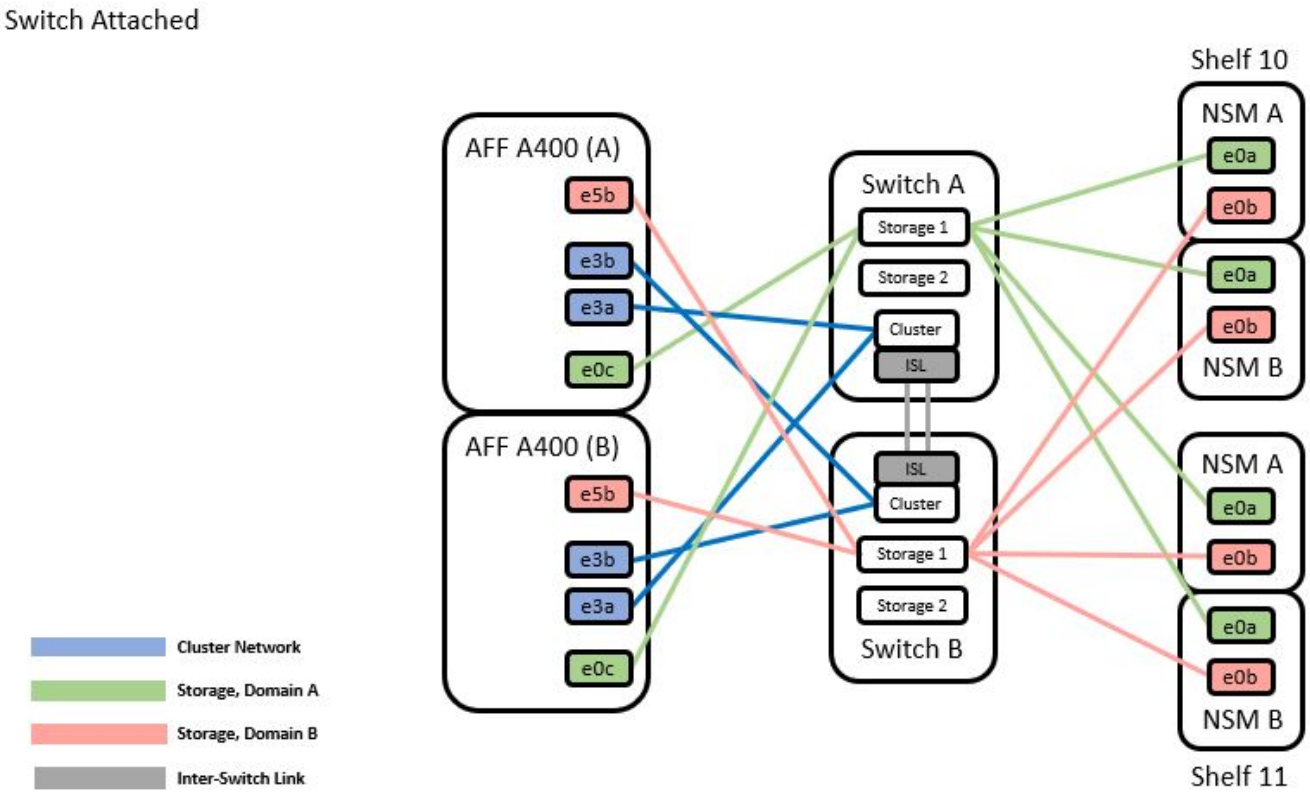
Instale o switch 9336C-FX2 e o painel de passagem em um gabinete NetApp , conforme necessário.

Complete a Planilha de cabeamento do Cisco Nexus 9336C-FX2

Use as seguintes imagens de cabeamento para concluir o cabeamento entre as controladoras e os switches.

Armazenamento do cabo NS224 como switch-anexado

Se você quiser o armazenamento do cabo NS224 como conetado ao switch, siga o diagrama anexado ao switch:

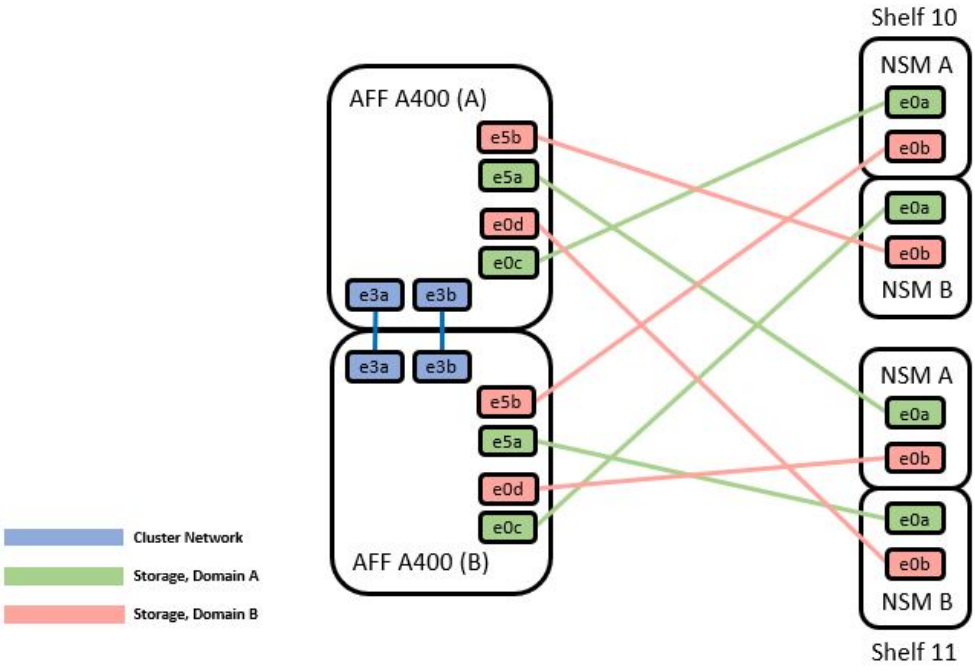


Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Armazenamento do cabo NS224 como conexão direta

Se você quiser fazer o armazenamento de NS224 GB por cabo como conexão direta em vez de usar as portas de armazenamento de switch compartilhado, siga o diagrama de conexão direta:

Direct Attached



	Port	Node
Path_A	e0c	Node_A
		Node_B
	e5a	Node_A
		Node_B
Path_B	e5b	Node_A
		Node_B
	e0d	Node_A
		Node_B

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Folha de cálculo do cabeamento Cisco Nexus 9336C-FX2

Se você quiser documentar as plataformas suportadas, você deve preencher a Planilha de cabeamento em branco usando a Planilha de cabeamento de amostra concluída como um guia.

A definição de porta de amostra em cada par de switches é a seguinte:

	Switch A			Switch B	
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1	Cluster	40/100GbE	1	Cluster	40/100GbE
2	Cluster	40/100GbE	2	Cluster	40/100GbE
3	Cluster	40/100GbE	3	Cluster	40/100GbE
4	Cluster	40/100GbE	4	Cluster	40/100GbE
5	Cluster	40/100GbE	5	Cluster	40/100GbE
6	Cluster	40/100GbE	6	Cluster	40/100GbE
7	Cluster	40/100GbE	7	Cluster	40/100GbE
8	Cluster	40/100GbE	8	Cluster	40/100GbE
9	Cluster	40GbE w/4x10GbE b/o	9	Cluster	40GbE w/4x10GbE b/o
10	Cluster	100GbE w/4x25GbE b/o	10	Cluster	100GbE w/4x25GbE b/o
11	Storage	100GbE	11	Storage	100GbE
12	Storage	100GbE	12	Storage	100GbE
13	Storage	100GbE	13	Storage	100GbE
14	Storage	100GbE	14	Storage	100GbE
15	Storage	100GbE	15	Storage	100GbE
16	Storage	100GbE	16	Storage	100GbE
17	Storage	100GbE	17	Storage	100GbE
18	Storage	100GbE	18	Storage	100GbE
19	Storage	100GbE	19	Storage	100GbE
20	Storage	100GbE	20	Storage	100GbE
21	Storage	100GbE	21	Storage	100GbE
22	Storage	100GbE	22	Storage	100GbE
23	Storage	100GbE	23	Storage	100GbE
24	Storage	100GbE	24	Storage	100GbE
25	Storage	100GbE	25	Storage	100GbE
26	Storage	100GbE	26	Storage	100GbE
27	Storage	100GbE	27	Storage	100GbE
28	Storage	100GbE	28	Storage	100GbE
29	Storage	100GbE	29	Storage	100GbE
30	Storage	100GbE	30	Storage	100GbE
31	Storage	100GbE	31	Storage	100GbE
32	Storage	100GbE	32	Storage	100GbE
33	Storage	100GbE	33	Storage	100GbE
34	Storage	100GbE	34	Storage	100GbE
35	ISL	100GbE	35	ISL	100GbE
36	ISL	100GbE	36	ISL	100GbE

Local:

- 100g ISL para mudar A porta 35
- 100g ISL para mudar A porta 36
- 100g ISL para a porta 35 do interrutor B.
- 100g ISL para a porta 36 do interrutor B.

Folha de cálculo de cablagem em branco

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A tabela conexões de cluster suportadas do Hardware Universe define as portas de cluster usadas pela plataforma.

	Switch A			Switch B	
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1			1		
2			2		
3			3		
4			4		
5			5		
6			6		
7			7		
8			8		
9			9		
10			10		
11			11		
12			12		
13			13		
14			14		
15			15		
16			16		
17			17		
18			18		
19			19		
20			20		
21			21		
22			22		
23			23		
24			24		
25			25		
26			26		
27			27		
28			28		
29			29		
30			30		
31			31		
32			32		
33			33		
34			34		
35			35		
36			36		

Local:

- 100g ISL para mudar A porta 35
- 100g ISL para mudar A porta 36
- 100g ISL para a porta 35 do interrutor B.
- 100g ISL para a porta 36 do interrutor B.

O que vem a seguir

"Instale o interrutor".

Instale os switches compartilhados Cisco Nexus 9336C-FX2

Siga estas instruções para configurar os switches compartilhados do Cisco Nexus 9336C-FX2.

Antes de começar

Certifique-se de que tem o seguinte:

- Documentação necessária do switch compartilhado, documentação do controlador e documentação do ONTAP. "Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2"Consulte e "Documentação do NetApp ONTAP".
- Licenças aplicáveis, informações de rede e configuração e cabos.
- Fichas de trabalho de cablagem concluídas. "Complete a Planilha de cabeamento do Cisco Nexus 9336C-FX2"Consulte . Para obter mais informações sobre cabeamento, consulte o "Hardware Universe".

Passos

1. Rack os switches, controladores e NS224 compartimentos de storage NVMe.

   Consulte o "Instruções de estantes" para saber como colocar o switch em rack em um gabinete NetApp.

2. Ligue os switches, as controladoras e as NS224 gavetas de storage NVMe.

O que se segue?

Opcionalmente, você pode"Instale um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp" . Caso contrário, vá para"Configure o interrutor" .

Instale um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp

Dependendo da sua configuração, você pode precisar instalar o switch Cisco Nexus 9336C-FX2 e o painel pass-through em um gabinete NetApp. Os suportes padrão estão incluídos com o interrutor.

Antes de começar

Certifique-se de que tem o seguinte:

- Para cada interrutor, você deve fornecer os oito parafusos 10-32 ou 12-24 e porcas de grampo para montar os suportes e trilhos deslizantes nos postes dianteiros e traseiros do gabinete.
- Você deve usar o kit de trilho padrão Cisco para instalar o switch em um gabinete NetApp.

> Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

Documentação necessária

Reveja os requisitos iniciais de preparação, o conteúdo do kit e as precauções de segurança no "Guia de instalação de hardware do Cisco Nexus 9000 Series".

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

   O kit de painel de passagem está disponível na NetApp (código de peça X8784-R6).

O kit do painel de passagem do NetApp contém o seguinte hardware:

- Um painel obturador de passagem
- Quatro parafusos 10-32 x .75
- Quatro porcas de freio 10-32

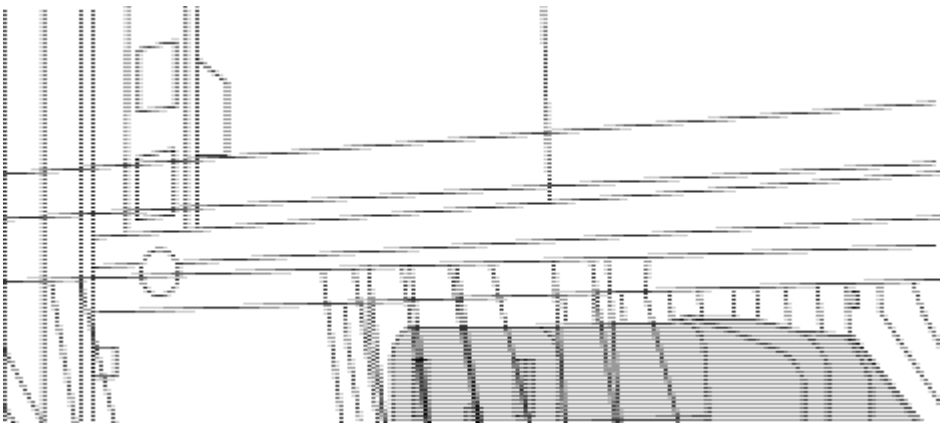
i. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

   Neste procedimento, o painel obturador será instalado em U40.

ii. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

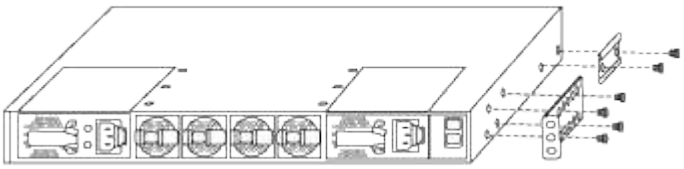
iii. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

iv. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.

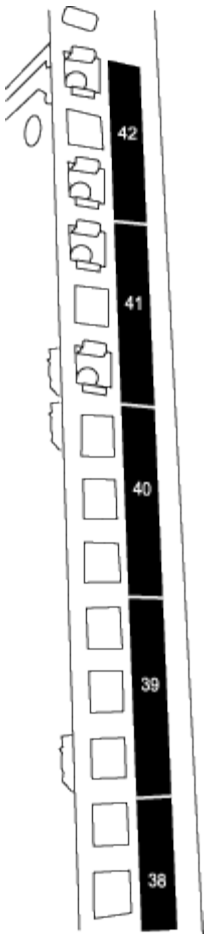


(1) conetor fêmea do cabo de ligação em ponte.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.
   a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.



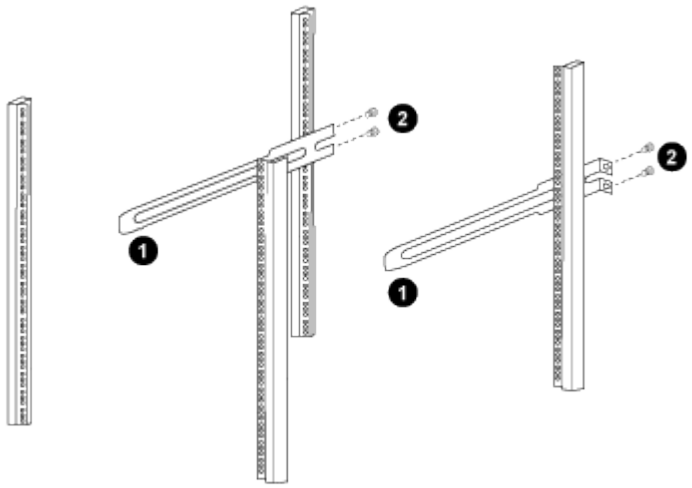
   b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.
   c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.
   d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.
3. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



Os dois interrutores 9336C-FX2 sempre serão montados no topo 2U do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no gabinete.

   a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



(1) enquanto desliza suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.

(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

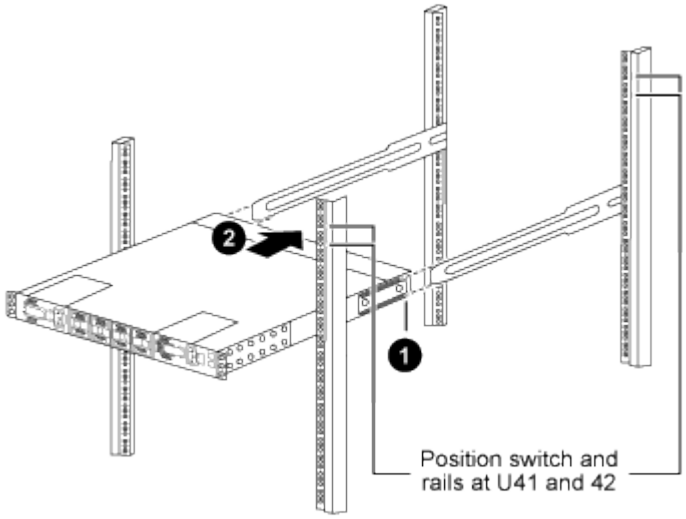
a. Repita o passo 4a para a coluna traseira do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

5. Instale o interrutor no gabinete.

> Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

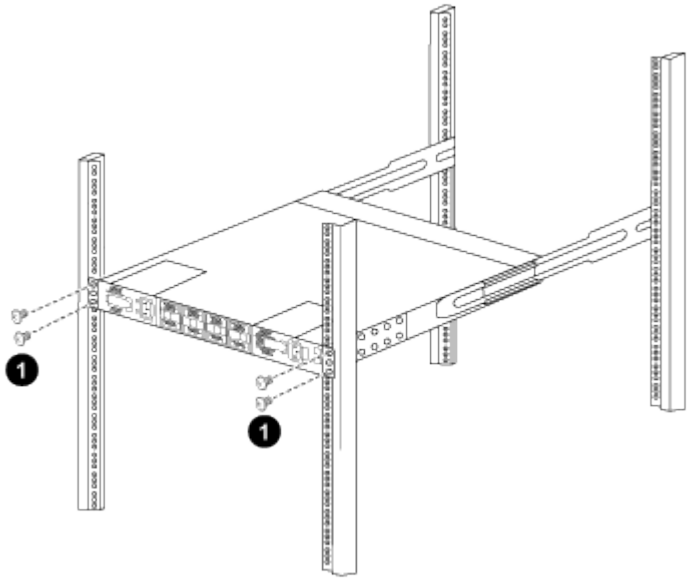
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário manter a frente do segundo interrutor durante o processo de instalação.

6. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
7. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

8. Conete a porta de gerenciamento de cada switch 9336C-FX2 a um dos switches de gerenciamento (se solicitado) ou conete-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

Configurar o software

Fluxo de trabalho de instalação de software para switches compartilhados Cisco Nexus 9336C-FX2

Para instalar e configurar o software para um switch compartilhado Cisco Nexus 9336C-FX2, siga estas etapas:

1. **"Configure o interrutor"**

Configure o switch compartilhado 9336C-FX2.

2. **"Prepare-se para instalar o software NX-os e o RCF"**

O software Cisco NX-OS e os arquivos de configuração de referência (RCFs) devem ser instalados nos switches compartilhados Cisco 9336C-FX2.

3. **"Instale ou atualize o software NX-os"**

Baixe e instale ou atualize o software NX-OS no switch compartilhado Cisco 9336C-FX2.

4. **"Instale o RCF"**

Instale o RCF após configurar o switch compartilhado Cisco 9336C-FX2 pela primeira vez.

5. **"Atualize seu RCF"**

Atualize sua versão do RCF quando tiver uma versão existente do arquivo RCF instalada em seus switches operacionais.

6 **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações do switch compartilhado 9336C-FX2.

Configurar os switches compartilhados Cisco Nexus 9336C-FX2

Siga estas instruções para configurar os switches compartilhados do Cisco Nexus 9336C-FX2.

Antes de começar

Certifique-se de que tem o seguinte:

- Documentação necessária do switch compartilhado, documentação do controlador e documentação do ONTAP. "Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2"Consulte e "Documentação do NetApp ONTAP".
- Licenças aplicáveis, informações de rede e configuração e cabos.
- Fichas de trabalho de cablagem concluídas. "Complete a Planilha de cabeamento do Cisco Nexus 9336C-FX2"Consulte . Para obter mais informações sobre cabeamento, consulte o "Hardware Universe".

Passos

1. execute uma configuração inicial dos switches.

   Para a configuração, você precisa do número e tipo apropriados de cabos e conetores de cabo para seus switches.

   Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de rede.

2. Arranque o interrutor.

   Forneça as respostas aplicáveis às seguintes perguntas de configuração inicial ao inicializar o switch pela primeira vez.

   A política de segurança do seu site define as respostas e os serviços a serem ativados.

   a. Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)

      Responda com **sim**. A predefinição é não

   b. Pretende aplicar o padrão de palavra-passe seguro? (sim/não)

      Responda com **sim**. O padrão é sim.

   c. Introduza a palavra-passe para admin.

      A senha padrão é admin; você deve criar uma nova senha forte.

      Uma senha fraca pode ser rejeitada.

d. Pretende introduzir a caixa de diálogo de configuração básica? (sim/não)

   Responda com **sim** na configuração inicial do comutador.

e. Criar outra conta de login? (sim/não)

   Sua resposta depende das políticas do seu site em administradores alternativos. A predefinição é não

f. Configurar string de comunidade SNMP somente leitura? (sim/não)

   Responda com **não**. A predefinição é não

g. Configurar string de comunidade SNMP de leitura-escrita? (sim/não)

   Responda com **não**. A predefinição é não

h. Introduza o nome do interrutor.

   O nome do switch está limitado a 63 carateres alfanuméricos.

i. Continuar com a configuração de gerenciamento fora da banda (mgmt0)? (sim/não)

   Responda com **yes** (o padrão) nesse prompt. No prompt mgmt0 IPv4 address:, insira seu endereço IP: ip_address

j. Configurar o gateway padrão? (sim/não)

   Responda com **sim**. No endereço IPv4 do prompt default-gateway:, digite seu default_gateway.

k. Configurar opções IP avançadas? (sim/não)

   Responda com **não**. A predefinição é não

l. Ativar o serviço telnet? (sim/não)

   Responda com **não**. A predefinição é não

m. Ativar serviço SSH? (sim/não)

   Responda com **sim**. O padrão é sim.

   O SSH é recomendado ao usar o Ethernet Switch Health Monitor (CSHM) para seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.

a. Digite o tipo de chave SSH que você deseja gerar (dsa/rsa/rsa1). O padrão é rsa.
b. Introduza o número de bits de chave (1024- 2048).
c. Configurar o servidor NTP? (sim/não)

   Responda com **não**. A predefinição é não

d. Configurar a camada de interface padrão (L3/L2):

   Responda com **L2**. A predefinição é L2.

e. Configurar o estado predefinido da interface da porta do switch (Shut/noshut):

   Responda com **noshut**. O padrão é noshut.

f. Configurar o perfil do sistema CoPP (strict/moderate/lenient/dense):

   Responda com **strict**. O padrão é rigoroso.

g. Pretende editar a configuração? (sim/não)

   Você deve ver a nova configuração neste momento. Reveja e faça as alterações necessárias à configuração que acabou de introduzir. Responda com não no prompt se você estiver satisfeito com a configuração. Responda com **yes** se quiser editar as configurações.

h. Utilizar esta configuração e guardá-la? (sim/não)

   Responda com **yes** para salvar a configuração. Isto atualiza automaticamente as imagens do Kickstart e do sistema.

3. Verifique as opções de configuração que você fez no visor que aparece no final da configuração e certifique-se de salvar a configuração.

   Se você não salvar a configuração nesta fase, nenhuma das alterações entrará em vigor na próxima vez que você reiniciar o switch.

4. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software suportada pelo NetApp para os switches a partir da "Transferência do software Cisco" página.

O que se segue?

"Prepare-se para instalar o NX-os e o RCF".

Prepare-se para instalar o software NX-os e o RCF

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Documentação sugerida

- "Página do switch Ethernet Cisco"

  Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

- "Guias de atualização e downgrade de software"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

- "Atualização do Cisco Nexus 9000 e 3000 e Matriz ISSU"

  Fornece informações sobre atualização/downgrade disruptiva para o software Cisco NX-os em switches Nexus 9000 Series com base em suas versões atuais e de destino.

  Na página, selecione **Atualização disruptiva** e selecione sua versão atual e liberação de destino na lista suspensa.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01 e cluster1-02.
- Os nomes de LIF de cluster são 02-01_clus1 e cluster1-01_clus2 para cluster1-01 e cluster1-02_clus1 e cluster1-02_clus2 para cluster1-cluster1.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

   onde x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   network device-discovery show -protocol cdp
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C

4 entries were displayed.
```

4. Verifique o status administrativo ou operacional de cada interface de cluster.
   a. Exibir os atributos da porta de rede:

```
network port show -ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Exibir informações sobre os LIFs:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o comando de reversão automática está ativado em todas as LIFs do cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

O que se segue?

"Instale o software NX-os".

Instale o software NX-os

Siga este procedimento para instalar o software NX-os no switch compartilhado Nexus 9336C-FX2.

Antes de começar, conclua o procedimento em "Prepare-se para instalar o NX-os e o RCF".

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- "Página do switch Ethernet Cisco"

  Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

- "Guias de atualização e downgrade de software"

  Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

- "Atualização do Cisco Nexus 9000 e 3000 e Matriz ISSU"

  Fornece informações sobre atualização/downgrade disruptiva para o software Cisco NX-os em switches Nexus 9000 Series com base em suas versões atuais e de destino.

Na página, selecione **Atualização disruptiva** e selecione sua versão atual e liberação de destino na lista suspensa.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são CS1 e CS2.
- Os nomes dos nós são cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- Os nomes de LIF do cluster são cluster1-01_clus1, cluster1-01_clus2, cluster1-03_clus2, cluster1-03_clus1 , cluster1-02_clus2, cluster1-02_clus1, cluster1-04_clus1 e cluster1-04_clus2.
- O `cluster1::*>` prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o comando ping para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch pode alcançar o servidor no endereço IP 172.19.2.1:

   ```
   cs2# ping 172.19.2.1 VRF management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

`system cluster-switch show -is-monitoring-enabled-operational true`

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Copie o software NX-os e as imagens EPLD para o switch Nexus 9336C-FX2.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.5.bin  /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time:  05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 02:28:31]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS



Compatibility check is done:
Module  Bootable  Impact          Install-type  Reason
------  --------  --------------- ------------  ---------
  1     yes       Disruptive      Reset         Default upgrade is
not hitless



Images will be upgraded according to following table:

Module   Image    Running-Version(pri:alt)                 New-
Version         Upg-Required
-------  -------- ---------------------------------------
-------------------- ------------
  1      nxos     9.3(4)                                   9.3(5)
yes
  1      bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)      yes
```

```
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.
```

9. Verifique a nova versão do software NX-os depois que o switch reiniciar:

   `show version`

Mostrar exemplo

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.3(5)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

10. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x17
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2

cs2# 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.
```

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

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x19
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
```

12. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -role cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
```

```
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

13. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

14. Repita os passos 6 a 13 para instalar o software NX-os no interrutor CS1.
15. Ative a reversão automática nos LIFs do cluster.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

16. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que se segue?

"Instale o RCF".

Instalar o ficheiro de configuração de referência (RCF)

Você pode instalar o arquivo de configuração de referência (RCF) depois de configurar o switch Nexus 9336C-FX2 pela primeira vez.

Antes de começar, conclua o procedimento em "Prepare-se para instalar o NX-os e o RCF".

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma ligação de consola ao interrutor. A conexão do console é opcional se você tiver acesso remoto ao switch.
- O switch CS1 e o switch CS2 são ativados e a configuração inicial do switch está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão NX-os pretendida foi instalada.
- As ligações entre interrutores (ISL) entre os interrutores estão ligadas.
- As portas do cluster de nós do ONTAP não estão conetadas.

Passo 1: Instale o RCF nos interrutores

1. Faça login no switch CS1 usando SSH ou usando um console serial.
2. Copie o RCF para o flash de inicialização do switch CS1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referência de comando Cisco Nexus 9000 Series NX-os".

   Mostrar exemplo

   Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS1:

   ```
   cs1# copy tftp: bootflash: vrf management
   Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
   Enter hostname for the tftp server: 172.22.201.50
   Trying to connect to tftp server......Connection to Server
   Established.
   TFTP get operation was successful
   Copy complete, now saving to disk (please wait)...
   ```

3. Aplique o RCF baixado anteriormente ao flash de inicialização.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referência de comando Cisco Nexus 9000 Series NX-os".

   Mostrar exemplo

   Este exemplo mostra o arquivo RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` sendo instalado no switch CS1:

   ```
   cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
   config echo-commands
   ```

4. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs1# show banner motd

******************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Nexus N9K-C9336C-FX2
* Filename : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : 10-23-2020
* Version  : v1.6
*
* Port Usage:
* Ports  1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports  4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports  7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
******************************************************************
**********
```

5. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

  A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.
7. Depois de verificar se as versões RCF e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

```
cs1# copy running-config startup-config
[########################################] 100% Copy complete
```

8. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

10. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

11. Emita o comando write erase para apagar a configuração salva atual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

12. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Interrutor de reinicialização CS1.

```
cs1# reload

This command will reboot the system. (y/n)? [n] y
```

14. Repita os passos 1 a 13 no switch cs2.
15. Conecte as portas do cluster de todos os nós do cluster ONTAP aos switches CS1 e CS2.

Etapa 2: Verifique as conexões do interrutor

1. Verifique se as portas do switch conetadas às portas do cluster estão **up**.

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

2. Verifique se os nós de cluster estão em suas VLANs de cluster corretas usando os seguintes comandos:

```
show vlan brief

show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

```
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         active    Eth1/11, Eth1/12,
Eth1/13
                                                  Eth1/14, Eth1/15,
Eth1/16
                                                  Eth1/17, Eth1/18,
Eth1/19
                                                  Eth1/20, Eth1/21,
Eth1/22
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34

cs1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
----------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
Eth1/9/1      1       trunking      --
Eth1/9/2      1       trunking      --
Eth1/9/3      1       trunking      --
Eth1/9/4      1       trunking      --
Eth1/10/1     1       trunking      --
Eth1/10/2     1       trunking      --
Eth1/10/3     1       trunking      --
Eth1/10/4     1       trunking      --
Eth1/11       33      trunking      --
```

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

```
Eth1/11       31,33
Eth1/12       31,33
Eth1/13       31,33
Eth1/14       31,33
Eth1/15       31,33
Eth1/16       31,33
Eth1/17       31,33
Eth1/18       31,33
Eth1/19       31,33
Eth1/20       31,33
Eth1/21       31,33
Eth1/22       31,33
Eth1/23       32,34
Eth1/24       32,34
Eth1/25       32,34
Eth1/26       32,34
Eth1/27       32,34
Eth1/28       32,34
Eth1/29       32,34
Eth1/30       32,34
Eth1/31       32,34
Eth1/32       32,34
Eth1/33       32,34
Eth1/34       32,34
Eth1/35       1
Eth1/36       1
Po1           1
..
..
..
..
..
```

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

3. Verifique se o ISL entre CS1 e CS2 está funcional:

```
show port-channel summary
```

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

Passo 3: Configure o cluster do ONTAP

A NetApp recomenda que você use o Gerenciador de sistemas para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e configuração de cluster, incluindo a atribuição de um endereço IP de gerenciamento de nós, a inicialização do cluster, a criação de um nível local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Aceda a "Configure o ONTAP em um novo cluster com o Gerenciador do sistema" para obter instruções de configuração.

O que se segue?

"Configurar o monitoramento de integridade do switch".

Atualize seu arquivo de configuração de referência (RCF)

Você atualiza sua versão RCF quando você tem uma versão existente do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual.
- Se você estiver atualizando sua versão do RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se você precisar alterar a configuração de inicialização para refletir as imagens de inicialização atuais, você deve fazê-lo antes de reaplicar o RCF para que a versão correta seja instanciada em futuras reinicializações.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Antes de instalar uma nova versão do software do switch e RCFs, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Passo 1: Prepare-se para a atualização

1. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show –role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90    N9K-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

3. Desative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
false
```

Etapa 2: Configurar portas

1. No switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

```
cs1(config)# interface eth1/1/1-2,eth1/7-8

cs1(config-if-range)# shutdown
```

> Certifique-se de encerrar **todas** portas de cluster conetadas para evitar quaisquer problemas de conexão de rede. Consulte o artigo da base de dados de Conhecimento "Nó fora do quórum ao migrar LIF do cluster durante a atualização do SO do switch" para obter mais detalhes.

2. Verifique se as LIFs de cluster falharam para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

   `network interface show -role cluster`

   Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
8 entries were displayed.
cluster1::*>
```

3. Verifique se o cluster está em bom estado:

   `cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

4. Se você ainda não fez isso, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

   ```
   show running-config
   ```

   a. Registre quaisquer adições personalizadas entre o atual running-config e o arquivo RCF em uso (como uma configuração SNMP para sua organização).

   b. Para NX-os 10,2 e posterior, use o `show diff running-config` comando para comparar com o arquivo RCF salvo no flash de inicialização. Caso contrário, use uma ferramenta de comparação ou comparação de terceiros.

5. Salve os detalhes básicos de configuração no arquivo write_erase.cfg no flash de inicialização.

   ```
   cs1# show run | i "username admin password" > bootflash:write_erase.cfg

   cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

   cs1# show run | section "switchname" >> bootflash:write_erase.cfg
   ```

6. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

   ```
   cs1# echo "hardware access-list tcam region ing-racl 1024" >>
   bootflash:write_erase.cfg

   cs1# echo "hardware access-list tcam region egr-racl 1024" >>
   bootflash:write_erase.cfg

   cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
   bootflash:write_erase.cfg
   ```

   Veja o artigo da Base de Conhecimento "Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

7. Verifique se o arquivo write_erase.cfg está preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Emita o comando write erase para apagar a configuração salva atual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

9. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Execute uma reinicialização do switch:

```
switch# reload

This command will reboot the system. (y/n)? [n] y
```

11. Depois que o endereço IP de gerenciamento for acessível novamente, faça login no switch através de SSH.

    Talvez seja necessário atualizar as entradas do arquivo host relacionadas às chaves SSH.

12. Copie o RCF para o flash de inicialização do switch CS1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 9000 Series NX-os" nos guias.

    Mostrar exemplo

    Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server......Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

13. Aplique o RCF baixado anteriormente ao flash de inicialização.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 9000 Series NX-os" nos guias.

Mostrar exemplo

Este exemplo mostra o arquivo RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` sendo instalado no switch CS1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

14. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs1# show banner motd

**********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Nexus N9K-C9336C-FX2
* Filename : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : 10-23-2020
* Version  : v1.6
*
* Port Usage:
* Ports  1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports  4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports  7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
**********************************************************************
**********
```

15. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

  A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

16. Reaplique quaisquer personalizações anteriores à configuração do switch.
17. Depois de verificar se as versões RCF, adições personalizadas e configurações de switch estão corretas, copie o arquivo running-config para o arquivo startup-config.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 9000 Series NX-os" nos guias.

    ```
    cs1# copy running-config startup-config

    [] 100% Copy complete
    ```

18. Interrutor de reinicialização CS1. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e eventos de portas de cluster down" relatados nos nós enquanto o switch for reinicializado.

    ```
    cs1# reload

    This command will reboot the system. (y/n)? [n] y
    ```

19. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

       ```
       network port show -role cluster
       ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ---------------
-----
cs1                         cluster-network    10.233.205.90    NX9-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    NX9-
```

```
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

20. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

21. Repita os passos 1 a 20 no interrutor CS2.
22. Ative a reversão automática nos LIFs do cluster.

    `cluster1::*> **network interface modify -vserver Cluster -lif * -auto-revert True**`

Etapa 3: Verifique a configuração da rede do cluster e a integridade do cluster

1. Verifique se as portas do switch conetadas às portas do cluster estão **up**.

   ```
   show interface brief
   ```

   Mostrar exemplo

   ```
   cs1# show interface brief | grep up
   .
   .
   Eth1/1/1      1       eth  access up      none
   10G(D) --
   Eth1/1/2      1       eth  access up      none
   10G(D) --
   Eth1/7        1       eth  trunk  up      none
   100G(D) --
   Eth1/8        1       eth  trunk  up      none
   100G(D) --
   .
   .
   ```

2. Verifique se os nós esperados ainda estão conetados:

   ```
   show cdp neighbors
   ```

Mostrar exemplo

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Verifique se os nós de cluster estão em suas VLANs de cluster corretas usando os seguintes comandos:

   `show vlan brief`

   `show interface trunk`

Mostrar exemplo

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

```
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         active    Eth1/11, Eth1/12,
Eth1/13
                                                  Eth1/14, Eth1/15,
Eth1/16
                                                  Eth1/17, Eth1/18,
Eth1/19
                                                  Eth1/20, Eth1/21,
Eth1/22
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34

cs1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
----------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
Eth1/9/1      1       trunking      --
Eth1/9/2      1       trunking      --
Eth1/9/3      1       trunking      --
Eth1/9/4      1       trunking      --
Eth1/10/1     1       trunking      --
Eth1/10/2     1       trunking      --
Eth1/10/3     1       trunking      --
Eth1/10/4     1       trunking      --
Eth1/11       33      trunking      --
```

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

```
Eth1/11       31,33
Eth1/12       31,33
Eth1/13       31,33
Eth1/14       31,33
Eth1/15       31,33
Eth1/16       31,33
Eth1/17       31,33
Eth1/18       31,33
Eth1/19       31,33
Eth1/20       31,33
Eth1/21       31,33
Eth1/22       31,33
Eth1/23       32,34
Eth1/24       32,34
Eth1/25       32,34
Eth1/26       32,34
Eth1/27       32,34
Eth1/28       32,34
Eth1/29       32,34
Eth1/30       32,34
Eth1/31       32,34
Eth1/32       32,34
Eth1/33       32,34
Eth1/34       32,34
Eth1/35       1
Eth1/36       1
Po1           1
..
..
..
..
..
```

Para obter detalhes específicos de uso de porta e VLAN, consulte a seção banner e notas importantes no RCF.

4. Verifique se o ISL entre CS1 e CS2 está funcional:

```
show port-channel summary
```

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

5. Verifique se os LIFs do cluster reverteram para sua porta inicial:

   `network interface show -role cluster`

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver vserver_name -lif lif_name`

6. Verifique se o cluster está em bom estado:

`cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------- -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

7. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Redefinir o switch compartilhado 9336C-FX2 para os padrões de fábrica

Para redefinir o switch compartilhado 9336C-FX2 para os padrões de fábrica, você deve

apagar as configurações do switch 9336C-FX2.

Sobre esta tarefa

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

Passos

1. Apagar a configuração existente:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Recarregue o software do switch:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   O sistema é reinicializado e entra no assistente de configuração. Durante a inicialização, se você receber o prompt “Abortar provisionamento automático e continuar com a configuração normal? (sim/não)[n]”, você deve responder **sim** para prosseguir.

Migrar switches

Migre de um cluster sem switch com storage de conexão direta

É possível migrar de um cluster sem switch com armazenamento de conexão direta adicionando dois novos switches compartilhados.

O procedimento usado depende se você tem duas portas de rede de cluster dedicadas em cada controlador ou uma única porta de cluster em cada controlador. O processo documentado funciona para todos os nós que usam portas óticas ou Twinax, mas não é suportado neste switch se os nós estiverem usando portas integradas 10Gb BASE-T RJ45 para as portas de cluster-rede.

A maioria dos sistemas requer duas portas de rede de cluster dedicadas em cada controlador. Consulte "Switches Ethernet Cisco" para obter mais informações.

Se você tiver um ambiente de cluster sem switch de dois nós existente, poderá migrar para um ambiente de cluster comutado de dois nós usando os switches Cisco Nexus 9336C-FX2 para permitir que você escale além de dois nós no cluster.

Rever os requisitos

Certifique-se de que:

- Para a configuração sem switch de dois nós:
  - A configuração sem switch de dois nós está corretamente configurada e funcionando.
  - Os nós estão executando o ONTAP 9.8 e posterior.
  - Todas as portas de cluster estão no estado **up**.
  - Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e em suas portas **home**.
- Para a configuração do switch Cisco Nexus 9336C-FX2:
  - Ambos os switches têm conetividade de rede de gerenciamento.
  - Existe acesso à consola aos interrutores do cluster.
  - As conexões de switch de nó para nó Nexus 9336C-FX2 e switch para switch usam cabos Twinax ou fibra.
  - O NetApp "Hardware Universe" contém mais informações sobre cabeamento.
  - Os cabos ISL (Inter-Switch Link) são conetados às portas 1/35 e 1/36 em ambos os switches 9336C-FX2.
- A personalização inicial dos switches 9336C-FX2 está concluída. Para que:
  - Os switches 9336C-FX2 estão executando a versão mais recente do software
  - Os ficheiros de configuração de referência (RCFs) foram aplicados aos comutadores
  - Qualquer personalização de site, como SMTP, SNMP e SSH, é configurada nos novos switches.

Migrar os switches

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches 9336C-FX2 são *CS1* e *CS2*.
- Os nomes dos SVMs do cluster são *node1* e *node2*.
- Os nomes dos LIFs são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.
- O prompt cluster1::*> indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *E3A* e *e3b*, de acordo com o controlador AFF A400. O "Hardware Universe" contém as informações mais recentes sobre as portas de cluster reais para as suas plataformas.

Etapa 1: Migre de um cluster sem switch com conexão direta

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`.

   onde x é a duração da janela de manutenção em horas.

A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

1. altere o nível de privilégio para avançado, inserindo y quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

2. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster CS1 e CS2. Não deve desativar as portas ISL.

   Mostrar exemplo

   O exemplo a seguir mostra que as portas 1 a 34 voltadas para o nó estão desativadas no switch CS1:

   ```
   cs1# config
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/1-34
   cs1(config-if-range)# shutdown
   ```

3. Verifique se o ISL e as portas físicas no ISL entre os dois switches 9336C-FX2 CS1 e CS2 estão acima nas portas 1/35 e 1/36:

   ```
   show port-channel summary
   ```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS1:

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS2:

```
       cs2# show port-channel summary
        Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

4. apresenta a lista de dispositivos vizinhos:

```
show cdp neighbors
```

Este comando fornece informações sobre os dispositivos que estão conetados ao sistema.

Mostrar exemplo

O exemplo a seguir lista os dispositivos vizinhos no switch CS1:

```
cs1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 2
```

O exemplo a seguir lista os dispositivos vizinhos no switch CS2:

```
cs2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1                Eth1/35        177    R S I s     N9K-C9336C
Eth1/35
cs1           )    Eth1/36        177    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 2
```

5. Verifique se todas as portas de cluster estão ativas:

```
network port show - ipspace Cluster
```

Cada porta deve ser exibida para Link e Healthy for Health Status.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1
                                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- ------------
---------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy
e3b       Cluster      Cluster          up   9000  auto/100000
healthy

Node: node2
                                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- ------------
---------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy
e3b       Cluster      Cluster          up   9000  auto/100000
healthy
4 entries were displayed.
```

6. Verifique se todas as LIFs de cluster estão ativas e operacionais:

`network interface show - vserver Cluster`

Cada LIF de cluster deve exibir True para `Is Home` e ter um Admin de Status/Oper de up/up.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
4 entries were displayed.
```

7. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

`network interface show - vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert
       Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true
4 entries were displayed.
```

8. Desconete o cabo da porta do cluster E3A no node1 e conete o E3A à porta 1 no switch do cluster CS1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.

   O NetApp "Hardware Universe" contém mais informações sobre cabeamento.

9. Desconete o cabo da porta de cluster E3A no node2 e conete o E3A à porta 2 no switch de cluster CS1,

usando o cabeamento apropriado suportado pelos switches 9336C-FX2.

10. Habilite todas as portas voltadas para o nó no switch de cluster CS1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão ativadas no switch CS1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

11. Verifique se todas as LIFs de cluster são **up**, operacionais e exibidas como True para `Is Home`:

`network interface show - vserver Cluster`

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs são **up** em node1 e node2 e que `Is Home` os resultados são **true**:

```
cluster1::*> network interface show -vserver Cluster
          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node
Port    Home
--------- ------------ ---------- ------------------ -----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1       e3a
true
          node1_clus2  up/up      169.254.49.125/16  node1       e3b
true
          node2_clus1  up/up      169.254.47.194/16  node2       e3a
true
          node2_clus2  up/up      169.254.19.183/16  node2       e3b
true
4 entries were displayed.
```

12. exibe informações sobre o status dos nós no cluster:

`cluster show`

Mostrar exemplo

O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
2 entries were displayed.
```

13. Desconete o cabo da porta do cluster e3b no node1 e conete o e3b à porta 1 no switch do cluster CS2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
14. Desconete o cabo da porta de cluster e3b no node2 e conete o e3b à porta 2 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
15. Habilite todas as portas voltadas para o nó no switch de cluster CS2.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão ativadas no switch CS2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

16. Verifique se todas as portas de cluster estão ativas:

```
network port show - ipspace Cluster
```

Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão em node1 e node2:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false
4 entries were displayed.
```

17. Verifique se todas as interfaces são exibidas verdadeiras para `Is Home`:

`network interface show - vserver Cluster`

Isso pode levar vários minutos para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs são **up** em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> network interface show -vserver Cluster
          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e3a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e3b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e3a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e3b
true
4 entries were displayed.
```

18. Verifique se ambos os nós têm uma conexão para cada switch:

```
show cdp neighbors
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
cs1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           AFFA400
e3a
node2              Eth1/2         133    H           AFFA400
e3a
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4
cs2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           AFFA400
e3b
node2              Eth1/2         133    H           AFFA400
e3b
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4
```

19. Mostre informações sobre os dispositivos de rede descobertos em seu cluster:

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2       /cdp
            e3a    cs1                       0/2               N9K-
C9336C
            e3b    cs2                       0/2               N9K-
C9336C

node1       /cdp
            e3a    cs1                       0/1               N9K-
C9336C
            e3b    cs2                       0/1               N9K-
C9336C
4 entries were displayed.
```

20. Verifique se a configuração de armazenamento do par HA 1 (e par HA 2) está correta e livre de erros:

`system switch ethernet show`

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type                  Address
Model
------------------------- --------------------- ---------------
----------
sh1
                          storage-network       172.17.227.5
C9336C

       Serial Number: FOC221206C2
        Is Monitored: true
              Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                      9.3(5)
      Version Source: CDP
sh2
                          storage-network       172.17.227.6
C9336C
       Serial Number: FOC220443LZ
        Is Monitored: true
              Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                      9.3(5)
      Version Source: CDP
2 entries were displayed.
storage::*>
```

21. Verifique se as configurações estão desativadas:

`network options switchless-cluster show`

> Pode demorar vários minutos para o comando ser concluído. Aguarde até que o anúncio "3 minutos de duração expire".

A `false` saída no exemplo a seguir mostra que as configurações estão desativadas:

Mostrar exemplo

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. Verifique o status dos membros do nó no cluster:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

23. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. altere o nível de privilégio de volta para admin:

```
set -privilege admin
```

Passo 2: Configure o switch compartilhado

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches compartilhados são *SH1* e *SH2*.
- Os nós são *node1* e *node2*.

> O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches, os comandos ONTAP são usados, a menos que indicado de outra forma.

1. Verifique se a configuração de armazenamento do par HA 1 (e par HA 2) está correta e sem erros:

```
system switch ethernet show
```

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type                  Address
Model
------------------------- --------------------  ---------------
-------
sh1
                          storage-network       172.17.227.5
C9336C

      Serial Number: FOC221206C2
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(5)
     Version Source: CDP
sh2
                          storage-network       172.17.227.6
C9336C
       Serial Number: FOC220443LZ
        Is Monitored: true
              Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                      9.3(5)
      Version Source: CDP
2 entries were displayed.
storage::*>
```

2. Verifique se as portas do nó de storage estão íntegras e operacionais:

   ```
   storage port show -port-type ENET
   ```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                    Speed
VLAN
Node    Port    Type    Mode        (Gb/s)      State      Status
ID
------- ------- ------- ---------- ----------- ---------- ----------
-----
node1
        e0c     ENET   storage          100      enabled  online
30
        e0d     ENET   storage          100      enabled  online
30
        e5a     ENET   storage          100      enabled  online
30
        e5b     ENET   storage          100      enabled  online
30

node2
        e0c     ENET  storage           100      enabled  online
30
        e0d     ENET  storage           100      enabled  online
30
        e5a     ENET  storage           100      enabled  online
30
        e5b     ENET  storage           100      enabled  online
30
```

3. mova as portas do par HA 1, NSM224 caminho A para o intervalo de portas SH1 11-22.
4. Instale um cabo do par HA 1, node1, caminho A até o intervalo de portas SH1 11-22. Por exemplo, o caminho Que uma porta de armazenamento em um AFF A400 é e0c.
5. Instale um cabo do par HA 1, node2, caminho A até o intervalo de portas SH1 11-22.
6. Verifique se as portas dos nós estão íntegras e operacionais:

   ```
   storage port show -port-type ENET
   ```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                    Speed
VLAN
Node    Port    Type    Mode       (Gb/s)      State      Status
ID
------- ------- ------- ---------- ----------- ---------- ----------
-----
node1
        e0c     ENET   storage          100      enabled  online
30
        e0d     ENET   storage            0      enabled  offline
30
        e5a     ENET   storage            0      enabled  offline
30
        e5b     ENET   storage          100      enabled  online
30

node2
        e0c     ENET  storage           100      enabled  online
30
        e0d     ENET  storage             0      enabled  offline
30
        e5a     ENET  storage             0      enabled  offline
30
        e5b     ENET  storage           100      enabled  online
30
```

7. Verifique se não há problemas de cabeamento ou switch de storage no cluster:

   `system health alert show -instance`

   Mostrar exemplo

   ```
   storage::*> system health alert show -instance
   There are no entries matching your query.
   ```

8. Mova o par de HA 1 portas de caminho B NSM224 para o intervalo de portas SH2 11-22.
9. Instale um cabo do par HA 1, node1, caminho B para o intervalo de portas SH2 11-22. Por exemplo, a porta de armazenamento de caminho B em um AFF A400 é e5b.
10. Instale um cabo do par HA 1, node2, caminho B para o intervalo de portas SH2 11-22.

11. Verifique se as portas dos nós estão íntegras e operacionais:

    `storage port show -port-type ENET`

    Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                  Speed
VLAN
Node    Port    Type    Mode       (Gb/s)      State      Status
ID
------- ------- ------- ---------- ----------- ---------- ----------
-----
node1
        e0c     ENET   storage          100      enabled  online
30
        e0d     ENET   storage            0      enabled  offline
30
        e5a     ENET   storage            0      enabled  offline
30
        e5b     ENET   storage          100      enabled  online
30

node2
        e0c     ENET  storage           100      enabled  online
30
        e0d     ENET  storage             0      enabled  offline
30
        e5a     ENET  storage             0      enabled  offline
30
        e5b     ENET  storage           100      enabled  online
30
```

12. Verifique se a configuração de armazenamento do par HA 1 está correta e sem erros:

    `system switch ethernet show`

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type                  Address
Model
------------------------- --------------------- ----------------
----------
sh1
                          storage-network       172.17.227.5
C9336C

      Serial Number: FOC221206C2
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(5)
     Version Source: CDP
sh2
                          storage-network       172.17.227.6
C9336C
      Serial Number: FOC220443LZ
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(5)
     Version Source: CDP
2 entries were displayed.
storage::*>
```

13. Reconfigure as portas de storage secundário não utilizadas (controladora) no par de HA 1 do storage à rede. Se mais de um NS224 foi conetado diretamente, haverá portas que devem ser reconfiguradas.

Mostrar exemplo

```
storage port modify –node [node name] –port [port name] –mode
network
```

Para colocar portas de armazenamento em um domínio de broadcast:

- `network port broadcast-domain create` (para criar um novo domínio, se necessário)
- `network port broadcast-domain add-ports` (para adicionar portas a um domínio existente)

14. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migrar de uma configuração comutada com storage com conexão direta

Você pode migrar de uma configuração comutada com armazenamento de conexão direta adicionando dois novos switches compartilhados.

Interrutores suportados

Os seguintes switches são suportados:

- Nexus 9336C-FX2
- Nexus 3232C

As versões ONTAP e NX-os suportadas neste procedimento estão na página switches Ethernet Cisco. "Switches Ethernet Cisco"Consulte .

Portas de ligação

Os switches usam as seguintes portas para se conetar a nós:

- Nexus 9336C-FX2P:
  - Portas 1- 3: Portas intra-cluster do modo de fuga (4x10G), int E1/1/1-4, E1/2/3-4, E1/1/1-4
  - Portas 4- 6: Portas intra-cluster/HA do modo de fuga (4x25G), int E1/4/1-4, E1/5/1-4, E1/6/1-4
  - Portas 7-34: Portas 40/100GbE intra-cluster/HA, int E1/7-34
- Nexus 3232CP:
  - Portas 1-30: 10/40/100 GbE
- Os switches usam as seguintes portas ISL (Inter-Switch Link):
  - Portas int E1/35-36: Nexus 9336C-FX2
  - Portas E1/31-32: Nexus 3232C

O "Hardware Universe" contém informações sobre o cabeamento suportado para todos os switches de cluster.

O que você vai precisar

- Certifique-se de que concluiu as seguintes tarefas:
  - Configurou algumas das portas nos switches Nexus 9336C-FX2 para serem executadas a 100 GbE.
  - Conectividade de 100 GbE planejada, migrada e documentada de nós para os switches Nexus 9336C-FX2.
  - Migração de outros switches de cluster Cisco sem interrupções de um cluster ONTAP para switches de rede Cisco Nexus 9336C-FX2.
- A rede de switch existente está corretamente configurada e funcionando.
- Todas as portas estão no estado **up** para garantir operações ininterruptas.
- Os switches Nexus 9336C-FX2 são configurados e operando sob a versão adequada do NX-os instalado

e o arquivo de configuração de referência (RCF) aplicado.

- A configuração de rede existente tem o seguinte:
  - Um cluster NetApp redundante e totalmente funcional usando ambos os switches Cisco mais antigos.
  - Conetividade de gerenciamento e acesso ao console aos switches Cisco mais antigos e aos novos switches.
  - Todas as LIFs de cluster no estado **up** com os LIFs de cluster estão em suas portas residenciais.
  - Portas ISL ativadas e cabeadas entre os outros switches Cisco e entre os novos switches.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de cluster Cisco Nexus 3232C existentes são *C1* e *C2*.
- Os novos switches Nexus 9336C-FX2 são *SH1* e *SH2*.
- Os nós são *node1* e *node2*.
- Os LIFs de cluster são *node1_clus1* e *node1_clus2* no nó 1 e *node2_clus1* e *node2_clus2* no nó 2 respetivamente.
- O interrutor C2 é substituído primeiro pelo interrutor SH2 e, em seguida, o interrutor C1 é substituído pelo interrutor SH1.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=x h
   ```

   Onde x é a duração da janela de manutenção em horas.

2. Verifique o status administrativo e operacional de cada porta de cluster.
3. Verifique se todas as portas do cluster estão ativas com um status de integridade:

   ```
   network port show –role cluster
   ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster
Node: node1

Ignore
                                             Speed(Mbps)  Health
Health
Port    IPspace   Broadcast Domain Link MTU  Admin/Ope    Status
Status
------- --------- ---------------- ---- ---- ------------ --------
------
e3a     Cluster   Cluster          up   9000  auto/100000 healthy
false
e3b     Cluster   Cluster          up   9000  auto/100000 healthy
false

Node: node2

Ignore
                                             Speed(Mbps) Health
Health
Port    IPspace   Broadcast Domain Link MTU  Admin/Oper  Status
Status
------- --------- ---------------- ---- ---- ----------- ---------
------
e3a     Cluster   Cluster          up   9000  auto/100000 healthy
false
e3b     Cluster   Cluster          up   9000  auto/100000 healthy
false
4 entries were displayed.
cluster1::*>
```

4. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
         Logical     Status     Network           Current
Current Is
Vserver  Interface   Admin/Oper Address/Mask      Node        Port
Home
-------  ----------- ---------- ----------------- -----------
------- ----
Cluster
        node1_clus1  up/up      169.254.3.4/23    node1       e3a
true
        node1_clus2  up/up      169.254.3.5/23    node1       e3b
true
        node2_clus1  up/up      169.254.3.8/23    node2       e3a
true
        node2_clus2  up/up      169.254.3.9/23    node2       e3b
true
4 entries were displayed.
cluster1::*>
```

5. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                    Type               Address          Model
------------------------- ------------------ ---------------- ------
sh1                       cluster-network    10.233.205.90    N9K-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
sh2                       cluster-network    10.233.205.91    N9K-
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

6. Desativar reversão automática nos LIFs do cluster.

Mostrar exemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

7. desligue o interrutor C2.

Mostrar exemplo

```
c2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c2(config)# interface ethernet <int range>
c2(config)# shutdown
```

8. Verifique se as LIFs de cluster migraram para as portas hospedadas no switch de cluster SH1:

   `network interface show -role cluster`

   Isso pode levar alguns segundos.

   Mostrar exemplo

```
cluster1::*> network interface show -role cluster
          Logical     Status     Network         Current
Current  Is
Vserver   Interface   Admin/Oper Address/Mask    Node          Port
Home
--------- ----------- ---------- --------------- ------------
-------- -----
Cluster
          node1_clus1 up/up      169.254.3.4/23  node1         e3a
true
          node1_clus2 up/up      169.254.3.5/23  node1         e3a
false
          node2_clus1 up/up      169.254.3.8/23  node2         e3a
true
          node2_clus2 up/up      169.254.3.9/23  node2         e3a
false
4 entries were displayed.
cluster1::*>
```

9. substitua o interrutor C2 pelo novo interrutor SH2 e volte a ligar o novo interrutor.
10. Verifique se as portas estão em backup no SH2. **Nota** que os LIFs ainda estão no interrutor C1.
11. Desligue o interrutor C1.

    Mostrar exemplo

```
c1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c1(config)# interface ethernet <int range>
c1(config)# shutdown
```

12. Verifique se as LIFs de cluster migraram para as portas hospedadas no switch de cluster SH2. Isso pode levar alguns segundos.

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
         Logical        Status     Network         Current   Current
Is
Vserver  Interface      Admin/Oper Address/Mask    Node      Port
Home
-------- -------------- ---------- --------------- --------- -------
----
Cluster
         node1_clus1    up/up      169.254.3.4/23  node1     e3a
true
         node1_clus2    up/up      169.254.3.5/23  node1     e3a
false
         node2_clus1    up/up      169.254.3.8/23  node2     e3a
true
         node2_clus2    up/up      169.254.3.9/23  node2     e3a
false
4 entries were displayed.
cluster1::*>
```

13. substitua o interrutor C1 pelo novo interrutor SH1 e volte a ligar o novo interrutor.
14. Verifique se as portas estão em backup no SH1. **Nota** que os LIFs ainda estão no interrutor C2.
15. Ativar a reversão automática nos LIFs do cluster:

Mostrar exemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

16. Verifique se o cluster está saudável:

```
cluster show
```

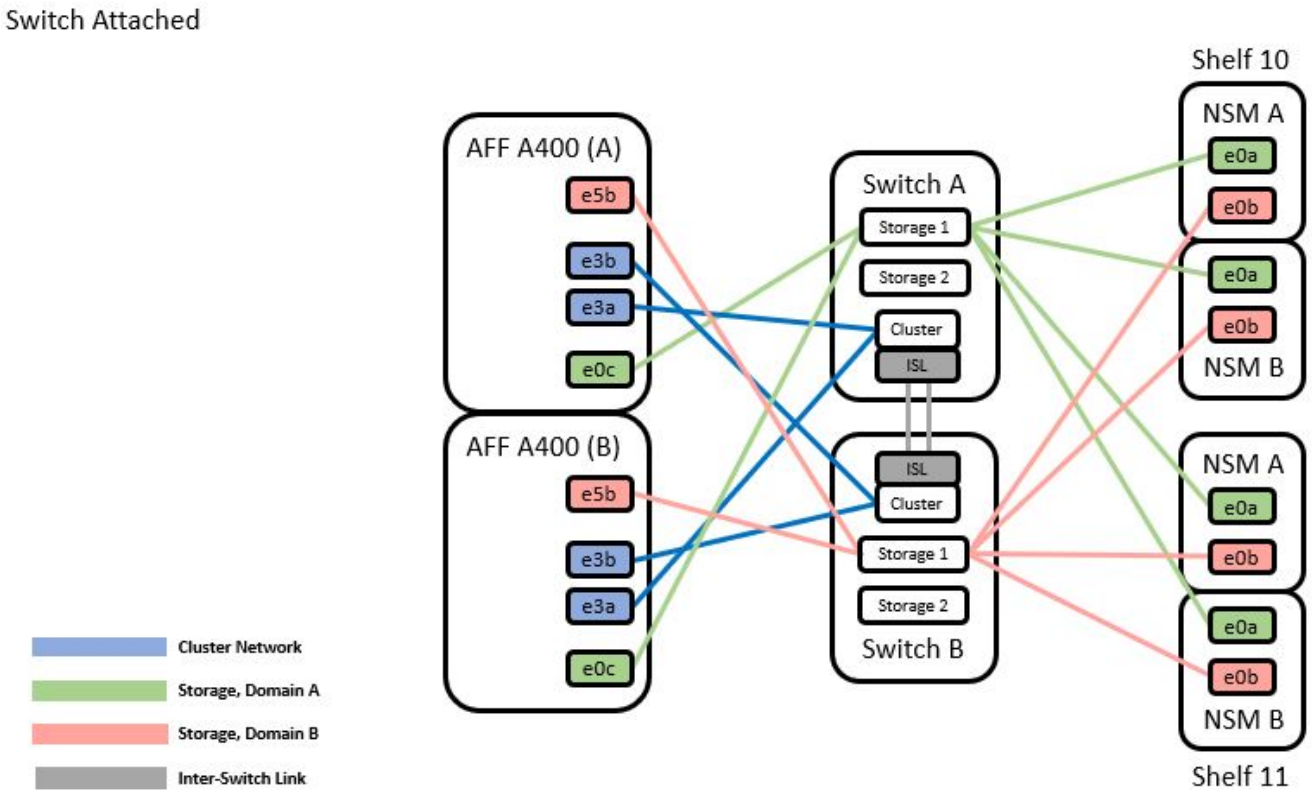
Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------- -------
node1                 true    true          false
node2                 true    true          false
2 entries were displayed.
cluster1::*>
```

Migre de uma configuração sem switch com storage conectado ao switch reutilizando os switches

É possível migrar de uma configuração sem switch com storage conectado ao switch reutilizando os switches de storage.

Ao reutilizar os switches de storage, os switches de storage do par de HA 1 se tornam os switches compartilhados, conforme mostrado na figura a seguir.



Passos

1. Verifique se a configuração de armazenamento do par HA 1 (e par HA 2) está correta e sem erros:

   ```
   system switch ethernet show
   ```

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type                  Address
Model
------------------------- --------------------- ----------------
----------
sh1
                          storage-network       172.17.227.5
C9336C

    Serial Number: FOC221206C2
     Is Monitored: true
           Reason: none
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(5)
   Version Source: CDP
sh2
                        storage-network        172.17.227.6
C9336C
    Serial Number: FOC220443LZ
     Is Monitored: true
           Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(5)
   Version Source: CDP
2 entries were displayed.
storage::*>
```

2. Verifique se as portas do nó estão íntegras e operacionais:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                     Speed
VLAN
Node    Port    Type    Mode       (Gb/s)    State     Status
ID
------- ------- ------- ---------- --------- --------- ---------
-----
node1
        e0c     ENET    storage          100 enabled   online
30
        e0d     ENET    storage          100 enabled   online
30
        e5a     ENET    storage          100 enabled   online
30
        e5b     ENET    storage          100 enabled   online
30

node2
        e0c     ENET    storage          100 enabled   online
30
        e0d     ENET    storage          100 enabled   online
30
        e5a     ENET    storage          100 enabled   online
30
        e5b     ENET    storage          100 enabled   online
30
```

3. mova os cabos do par HA 1, NSM224 caminho A do switch de armazenamento A para as portas de armazenamento NS224 partilhadas para o par HA 1, caminho A no switch de armazenamento A..
4. Mova o cabo do par de HA 1, nó A, caminho A para a porta de storage compartilhado do par de HA 1, nó A no switch de storage A.
5. Mova o cabo do par de HA 1, nó B, caminho A para a porta de storage compartilhado para o par de HA 1, nó B no switch de storage A.
6. Verifique se o storage anexado ao par HA 1, o switch de storage A está funcionando:

   ```
   system health alert show -instance
   ```

Mostrar exemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

7. substitua o RCF de armazenamento no switch compartilhado A pelo arquivo RCF compartilhado. "Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2"Consulte para obter mais detalhes.
8. Verifique se o storage conetado ao par HA 1, o switch de storage B está funcionando:

   `system health alert show -instance`

   Mostrar exemplo

   ```
   storage::*> system health alert show -instance
   There are no entries matching your query.
   ```

9. mova os cabos do par HA 1, NSM224 caminho B do switch de armazenamento B para as portas de armazenamento NS224 compartilhadas para o par HA 1, caminho B para o switch de armazenamento B.
10. Mova o cabo do par de HA 1, nó A, caminho B para a porta de storage compartilhado para o par de HA 1, nó A, caminho B no switch de storage B.
11. Mova o cabo do par de HA 1, nó B, caminho B para a porta de storage compartilhado para o par de HA 1, nó B, caminho B no switch de storage B.
12. Verifique se o storage conetado ao par HA 1, o switch de storage B está funcionando:

    `system health alert show -instance`

    Mostrar exemplo

    ```
    storage::*> system health alert show -instance
    There are no entries matching your query.
    ```

13. substitua o arquivo RCF de armazenamento no switch compartilhado B pelo arquivo RCF compartilhado. "Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2"Consulte para obter mais detalhes.
14. Verifique se o storage conetado ao par HA 1, o switch de storage B está funcionando:

    `system health alert show -instance`

Mostrar exemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

15. instale os ISLs entre o switch compartilhado A e o switch compartilhado B:

Mostrar exemplo

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# interface e1/35-36
sh1 (config-if-range)# no lldp transmit
sh1 (config-if-range)# no lldp receive
sh1 (config-if-range)# switchport mode trunk
sh1 (config-if-range)# no spanning-tree bpduguard enable
sh1 (config-if-range)# channel-group 101 mode active
sh1 (config-if-range)# exit
sh1 (config)# interface port-channel 101
sh1 (config-if)# switchport mode trunk
sh1 (config-if)# spanning-tree port type network
sh1 (config-if)# exit
sh1 (config)# exit
```

16. Converta o par HA 1 de um cluster sem switch para um cluster comutado. Use as atribuições de portas de cluster definidas pelo RCF compartilhado. "Instalar o software NX-os e arquivos de configuração de referência (RCFs)"Consulte para obter mais detalhes.

17. Verifique se a configuração de rede comutada é válida:

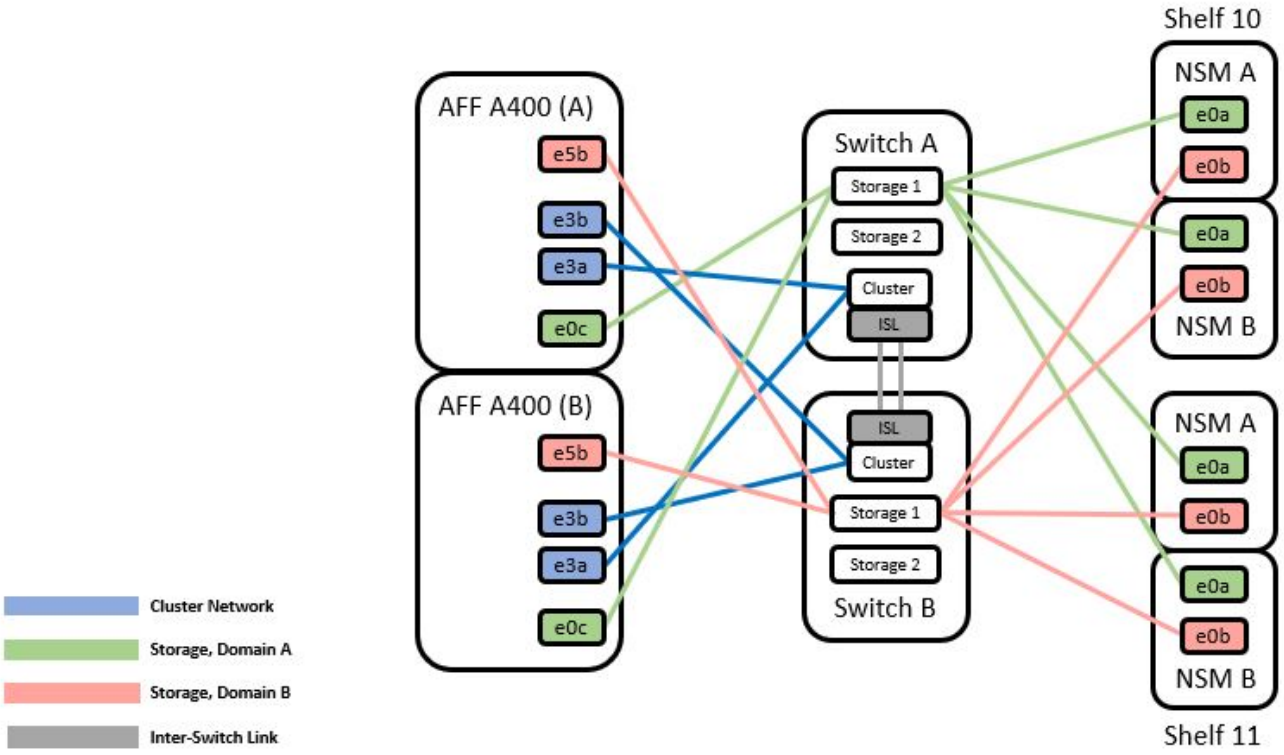
```
network port show
```

Migre de um cluster comutado com storage conectado a switch

É possível migrar de um cluster comutado com storage conectado ao switch reutilizando os switches.

Ao reutilizar os switches de storage, os switches de storage do par de HA 1 se tornam os switches compartilhados, conforme mostrado na figura a seguir.

Switch Attached



Passos

1. Verifique se a configuração de armazenamento do par HA 1 (e par HA 2) está correta e sem erros:

   ```
   system switch ethernet show
   ```

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type               Address          Model
------------------------- ------------------ ----------------
----------
sh1
                          storage-network    172.17.227.5     C9336C

     Serial Number: FOC221206C2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
       Version Source: CDP
sh2
                          storage-network    172.17.227.6     C9336C
     Serial Number: FOC220443LZ
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
2 entries were displayed.
storage::*>
```

2. mova os cabos do par HA 1, NSM224 caminho A do switch de armazenamento A para as NSM224 portas de armazenamento para o par HA 1, caminho A no switch de armazenamento A.
3. Mova o cabo do par de HA 1, nó A, caminho A para a porta de storage NSM224 para o par de HA 1, nó A no switch de storage A.
4. Mova o cabo do par de HA 1, nó B, caminho A para a porta de storage NSM224 para o par de HA 1, nó B no switch de storage A.
5. Verifique se o storage anexado ao par HA 1, o switch de storage A está funcionando:

   ```
   storage port show -port-type ENET
   ```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                    Speed
VLAN
Node    Port    Type    Mode        (Gb/s)       State     Status
ID
------- ------- ------- ---------- ------------ --------- ---------
-----
node1
        e0c     ENET    storage            100  enabled   online
30
        e0d     ENET    storage            100  enabled   online
30
        e5a     ENET    storage            100  enabled   online
30
        e5b     ENET    storage            100  enabled   online
30

node2
        e0c     ENET    storage            100  enabled   online
30
        e0d     ENET    storage            100  enabled   online
30
        e5a     ENET    storage            100  enabled   online
30
        e5b     ENET    storage            100  enabled   online
30
```

6. substitua o RCF de armazenamento no switch compartilhado A pelo arquivo RCF compartilhado. "Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2"Consulte para obter mais detalhes.
7. Verifique se o storage anexado ao par HA 1, o switch de storage A está funcionando:

   `system health alert show -instance`

Mostrar exemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

8. mova os cabos do par HA 1, NSM224 caminho B do switch de armazenamento B para as portas de armazenamento NS224 compartilhadas para o par HA 1, caminho B para o switch de armazenamento B.
9. Mova o cabo do par de HA 1, nó A, caminho B para a porta de storage compartilhado para o par de HA 1,

nó A, caminho B no switch de storage B.

10. Mova o cabo do par de HA 1, nó B, caminho B para a porta de storage compartilhado para o par de HA 1, nó B, caminho B no switch de storage B.
11. Verifique se o storage conetado ao par HA 1, o switch de storage B está funcionando:

    `system health alert show -instance`

    Mostrar exemplo

    ```
    storage::*> system health alert show -instance
    There are no entries matching your query.
    ```

12. substitua o arquivo RCF de armazenamento no switch compartilhado B pelo arquivo RCF compartilhado. "Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2"Consulte para obter mais detalhes.
13. Verifique se o storage conetado ao par HA 1, o switch de storage B está funcionando:

    `system health alert show -instance`

    Mostrar exemplo

    ```
    storage::*> system health alert show -instance
    There are no entries matching your query.
    ```

14. Verifique se a configuração de armazenamento do par HA 1 está correta e livre de erros:

    `system switch ethernet show`

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                    Type                 Address
Model
------------------------- -------------------- ----------------
----------
sh1
                          storage-network      172.17.227.5
C9336C

    Serial Number: FOC221206C2
     Is Monitored: true
           Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(5)
   Version Source: CDP
sh2
                          storage-network      172.17.227.6
C9336C
    Serial Number: FOC220443LZ
     Is Monitored: true
           Reason: None
 Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                   9.3(5)
   Version Source: CDP
2 entries were displayed.
storage::*>
```

15. instale os ISLs entre o switch compartilhado A e o switch compartilhado B:

Mostrar exemplo

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# interface e1/35-36*
sh1 (config-if-range)# no lldp transmit
sh1 (config-if-range)# no lldp receive
sh1 (config-if-range)# switchport mode trunk
sh1 (config-if-range)# no spanning-tree bpduguard enable
sh1 (config-if-range)# channel-group 101 mode active
sh1 (config-if-range)# exit
sh1 (config)# interface port-channel 101
sh1 (config-if)# switchport mode trunk
sh1 (config-if)# spanning-tree port type network
sh1 (config-if)# exit
sh1 (config)# exit
```

16. migre a rede do cluster dos switches de cluster existentes para os switches compartilhados usando o procedimento de substituição do switch e o RCF compartilhado. O novo switch compartilhado A é "CS1". O novo interrutor partilhado B é "CS2". "Substitua um switch compartilhado Cisco Nexus 9336C-FX2"Consulte e "Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2" para obter mais detalhes.
17. Verifique se a configuração de rede comutada é válida:

    ```
    network port show
    ```

18. Retire os interrutores do grupo de instrumentos não utilizados.
19. Retire os interrutores de armazenamento não utilizados.

Substitua um switch compartilhado Cisco Nexus 9336C-FX2

Você pode substituir um switch compartilhado Nexus 9336C-FX2 com defeito. Este é um procedimento sem interrupções (NDU).

Antes de começar

Antes de efetuar a substituição do interrutor, certifique-se de que:

- No cluster existente e infra-estrutura de rede:
  - O cluster existente é verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
  - Todas as portas de cluster são **up**.
  - Todas as interfaces lógicas de cluster (LIFs) são **up** e em suas portas domésticas.
  - O comando ping-cluster -nó node1 do cluster do ONTAP deve indicar que a conetividade básica e a comunicação maior do que a PMTU são bem-sucedidas em todos os caminhos.
- Para o interrutor de substituição Nexus 9336C-FX2:

- A conetividade de rede de gerenciamento no switch de substituição está funcional.
- O acesso do console ao interrutor de substituição está no lugar.
- As conexões de nó são as portas 1/1 a 1/34:
- Todas as portas ISL (Inter-Switch Link) estão desativadas nas portas 1/35 e 1/36.
- O arquivo de configuração de referência desejado (RCF) e o interrutor de imagem do sistema operacional NX-os são carregados no switch.
- Quaisquer personalizações de sites anteriores, como STP, SNMP e SSH, devem ser copiadas para o novo switch.

Sobre os exemplos

Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches Nexus 9336C-FX2 existentes são *SH1* e *SH2*.
- O nome dos novos switches Nexus 9336C-FX2 são *newsh1* e *newsh2*.
- Os nomes dos nós são *node1* e *node2*.
- As portas de cluster em cada nó são chamadas *E3A* e *e3b*.
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.
- O prompt para alterações em todos os nós de cluster é cluster1::*>.

O seguinte procedimento baseia-se na seguinte topologia de rede:

Mostrar exemplo de topologia

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper   Status
Status
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps)  Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper   Status
Status
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false
4 entries were displayed.


cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e3a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e3b
true
```

```
            node2_clus1  up/up    169.254.47.194/16  node2         e3a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e3b
true
4 entries were displayed.

cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e3a    sh1                       Eth1/2            N9K-
C9336C
            e3b    sh2                       Eth1/2            N9K-
C9336C

node1      /cdp
            e3a    sh1                       Eth1/1            N9K-
C9336C
            e3b    sh2                       Eth1/1            N9K-
C9336C
4 entries were displayed.

sh1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e3a
node2              Eth1/2         145    H           FAS2980       e3a
sh2                Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
sh2 (FDO220329V5)   Eth1/36       176    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4

sh2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
```

```
node1                Eth1/1          139    H           FAS2980       eb
node2                Eth1/2          124    H           FAS2980       eb
sh1                  Eth1/35         178    R S I s     N9K-C9336C
Eth1/35
sh1                  Eth1/36         178    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4
```

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   Onde x é a duração da janela de manutenção em horas.

2. Opcional: Instale o RCF e a imagem apropriados no interrutor, newsh2, e faça os preparativos necessários para o local.

   a. Se necessário, verifique, baixe e instale as versões apropriadas do software RCF e NX-os para o novo switch. Se você tiver verificado que o novo switch está corretamente configurado e não precisa de atualizações para o software RCF e NX-os, continue para Passo 3.

   b. Vá para a página Descrição do arquivo de configuração de referência do cluster e gerenciamento de switches de rede do NetApp no site de suporte da NetApp.

   c. Clique no link da Matriz de Compatibilidade de rede de Cluster e rede de Gerenciamento e anote a versão necessária do software do switch.

   d. Clique na seta para trás do navegador para retornar à página Descrição, clique EM CONTINUAR, aceite o contrato de licença e vá para a página Download.

   e. Siga as etapas na página Download para baixar os arquivos RCF e NX-os corretos para a versão do software ONTAP que você está instalando.

3. no novo switch, faça login como admin e encerre todas as portas que serão conetadas às interfaces do cluster de nós (portas 1/1 a 1/34). Se o interrutor que você está substituindo não estiver funcional e estiver desligado, vá para Passo 4. As LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

   Mostrar exemplo

   ```
   newsh2# config
   Enter configuration commands, one per line. End with CNTL/Z.
   newsh2(config)# interface e1/1-34
   newsh2(config-if-range)# shutdown
   ```

4. Verifique se todas as LIFs do cluster têm a reversão automática ativada.

   ```
   network interface show - vserver Cluster -fields auto-revert
   ```

Mostrar exemplo

```
cluster1::> network interface show -vserver Cluster -fields auto-
revert
             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true
4 entries were displayed.
```

5. Verifique a conetividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. desligue as portas ISL 1/35 e 1/36 no switch Nexus 9336C-FX2 SH1.

Mostrar exemplo

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1(config)# interface e1/35-36
sh1(config-if-range)# shutdown
```

2. Remova todos os cabos do switch Nexus 9336C-FX2 SH2 e, em seguida, conete-os às mesmas portas no switch Nexus C9336C-FX2 newsh2.
3. Abra as portas ISLs 1/35 e 1/36 entre os switches SH1 e newsh2 e verifique o status da operação do canal da porta.

   O Canal de porta deve indicar PO1(SU) e os portos Membros devem indicar eth1/35(P) e eth1/36(P).

Mostrar exemplo

Este exemplo ativa as portas ISL 1/35 e 1/36 e exibe o resumo do canal da porta no switch SH1.

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# int e1/35-36
sh1 (config-if-range)# no shutdown
sh1 (config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member       Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

sh1 (config-if-range)#
```

4. Verifique se a porta e3b está ativa em todos os nós:

```
network port show ipspace Cluster
```

Mostrar exemplo

A saída deve ser como o seguinte:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- ---------- - -
-------- ----
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- ----------- -
-------- ----
e3a       Cluster      Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/auto    -
false
4 entries were displayed.
```

5. no mesmo nó que você usou na etapa anterior, reverta o LIF de cluster associado à porta na etapa anterior usando o comando de reversão de interface de rede.

   Neste exemplo, LIF node1_clus2 no node1 é revertido com sucesso se o valor Casa for verdadeiro e a porta for e3b.

   Os comandos a seguir retornam LIF node1_clus2 em node1 para a porta inicial E3A e exibe informações sobre os LIFs em ambos os nós. Abrir o primeiro nó é bem-sucedido se a coluna is Home for **true** para ambas as interfaces de cluster e eles mostrarem as atribuições de porta corretas, neste exemplo E3A e e3b em node1.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3a     false
4 entries were displayed.
```

6. Exibir informações sobre os nós em um cluster:

```
cluster show
```

Mostrar exemplo

Este exemplo mostra que a integridade do nó para node1 e node2 neste cluster é verdadeira:

```
cluster1::*> cluster show
Node          Health  Eligibility
------------- ------- ------------
node1         false   true
node2         true    true
```

7. Verifique se todas as portas de cluster físico estão ativas:

```
network port show ipspace Cluster
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node node1
Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- ------------
-------- ------
e3a       Cluster     Cluster           up    9000  auto/100000
healthy  false
e3b       Cluster     Cluster           up    9000  auto/100000
healthy  false

Node: node2

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- ------------
-------- ------
e3a       Cluster      Cluster          up    9000  auto/100000
healthy  false
e3b       Cluster      Cluster          up    9000  auto/100000
healthy  false
4 entries were displayed.
```

8. Verifique a conetividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Confirme a seguinte configuração de rede de cluster:

```
network port show
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ----------- ---------------- ---- ----- ------------
-------- ------
e3a       Cluster     Cluster          up   9000  auto/100000
healthy  false
e3b       Cluster     Cluster          up   9000  auto/100000
healthy  false

Node: node2

Ignore
                                         Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- ------------
-------- ------
e3a       Cluster      Cluster          up   9000 auto/100000
healthy  false
e3b       Cluster      Cluster          up   9000 auto/100000
healthy  false
4 entries were displayed.

cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
```

```
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
4 entries were displayed.

cluster1::> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------ ----------------
----------------
node2      /cdp
            e3a    sh1    0/2               N9K-C9336C
            e3b    newsh2                    0/2               N9K-
C9336C
node1      /cdp
            e3a    sh1                       0/1               N9K-
C9336C
            e3b    newsh2                    0/1               N9K-
C9336C
4 entries were displayed.

sh1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e3a
node2                Eth1/2         145    H           FAS2980
e3a
newsh2               Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
newsh2               Eth1/36        176    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4

sh2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
```

```
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e3b
node2              Eth1/2         124    H           FAS2980
eb
sh1                Eth1/35        178    R S I s     N9K-C9336C
Eth1/35
sh1                Eth1/36        178    R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4
```

2. mova as portas de armazenamento do antigo switch SH2 para o novo switch newsh2.
3. Verifique se o storage anexado ao par de HA 1, o switch compartilhado newsh2 está funcionando.
4. Verifique se o storage anexado ao par HA 2, o switch compartilhado newsh2 está funcionando:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
                                     Speed
VLAN
Node    Port    Type    Mode       (Gb/s)      State     Status
ID
------- ------- ------- ---------- ----------- --------- ---------
-----
node1
        e3a     ENET    storage          100   enabled   online
30
        e3b     ENET    storage            0   enabled   offline
30
        e7a     ENET    storage            0   enabled   offline
30
        e7b     ENET    storage          100   enabled   online
30

node2
        e3a     ENET    storage          100   enabled   online
30
        e3b     ENET    storage            0   enabled   offline
30
        e7a     ENET    storage            0   enabled   offline
30
        e7b     ENET    storage          100   enabled   online
30
```

5. Verifique se as prateleiras estão cabeadas corretamente:

```
storage shelf port show -fields remote- device,remote-port
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-device,remote-
port
shelf id remote-port  remote-device
----- -- ------------ ----------------------------
3.20  0  Ethernet1/13 sh1
3.20  1  Ethernet1/13 newsh2
3.20  2  Ethernet1/14 sh1
3.20  3  Ethernet1/14 newsh2
3.30  0  Ethernet1/15 sh1
3.30  1  Ethernet1/15 newsh2
3.30  2  Ethernet1/16 sh1
3.30  3  Ethernet1/16 newsh2
8 entries were displayed.
```

6. Remova o interrutor antigo SH2.
7. Repita estes passos para o interrutor SH1 e para o novo interrutor newsh1.
8. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Monitorar a integridade do interrutor

Visão geral do monitor de integridade do interrutor

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.

Configurar o monitoramento de integridade do switch

Visão geral da configuração

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.

- "Configurar a coleção de registos"
- "Opcional: Configurar SNMPv3"

Configurar a coleção de registos

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 interrutor tem de estar ativada para o interrutor. 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
                                          Periodic    Periodic
Support
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.

O que se segue?

"Configurar SNMPv3 (opcional)".

Opcional: Configure o SNMPv3 para o seu switch

O SNMP é usado para monitorar os switches. O monitoramento por SNMPv3 é configurado seguindo este procedimento.

O CSHM (Ethernet Switch Health Monitor) utiliza SNMP para monitorar a integridade e o desempenho dos switches de cluster e armazenamento. Por predefinição, o SNMPv2c é configurado automaticamente através do ficheiro de configuração de referência (RCF). O SNMPv3 é mais seguro do que o SNMPv2 porque introduz recursos de segurança robustos, como autenticação, criptografia e integridade de mensagens, que protegem contra acesso não autorizado e garantem a confidencialidade e integridade dos dados durante a transmissão.

- 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

1. 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 cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! 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: cshm1!
                                 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-LLDP 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-LLDP 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

1. 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$94d69b56e921aec1790844eb53e772bf
state                 enabled
cumulus@sw1:~$
```

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: 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-LLDP 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
```

Verifique a integridade do interrutor

Visão geral da verificação de integridade

Os monitores de integridade monitoram proativamente certas condições críticas no cluster e emitem alertas se detetarem uma falha ou risco.

Para visualizar os alertas do monitor de integridade do switch Ethernet atualmente levantados, execute o comando: `system health alert show -monitor ethernet-switch`

Para exibir os alertas disponíveis do monitor de integridade do switch Ethernet, execute o comando: `system health alert definition show -monitor ethernet-switch`

Gerenciar o monitoramento de switches Ethernet

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 interrutor na configuração, como durante a manutenção.

Crie uma entrada de switch para que o ONTAP possa monitorá-la

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 interrutor

Se você quiser pausar ou parar o monitoramento de um determinado switch, mas ainda mantê-lo para monitoramento futuro, modifique seu `is-monitoring-enabled-admim` 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 interrutor 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.
```

Verifique o monitoramento dos switches Ethernet

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 conetados

Para confirmar se os switches Ethernet conetados 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 carateres 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 conetada à rede de gerenciamento.

Uma conexão de porta de gerenciamento correta é necessária para que o ONTAP execute consultas SNMP e

coleta de logs.

Solucionar problemas de alertas

Os alertas são emitidos se for detetada uma falha, risco ou condição crítica para um switch Ethernet no cluster.

Se existirem alertas enviados, o estado de funcionamento do sistema comunica um estado degradado para o cluster. Os alertas levantados incluem as informações de que você precisa para responder à integridade degradada do sistema.

Para exibir os alertas disponíveis do monitor de integridade do switch Ethernet, execute o comando: `system health alert definition show -monitor ethernet-switch`

Consulte o artigo da base de dados de Conhecimento "Mudar o Guia de resolução de alertas do Monitor de Saúde" para obter detalhes de resolução avançada de alertas.

Recolha de registos

Descrição geral da coleção de registos

Com a configuração de coleta de logs, você pode habilitar uma coleta por hora de dados periódicos coletados pelo AutoSupport e solicitar Registros de suporte detalhados.

"Configurar a coleção de registos"Consulte para obter mais detalhes.

Solucionar problemas na coleta de logs

Se você encontrar algum dos seguintes status de erro relatados pelo recurso de coleta de log (visível na saída do `system switch ethernet log show` comando), tente as etapas de depuração correspondentes:

Estado do erro de recolha de registos	Resolução
Chaves RSA não presentes	Regenerar chaves SSH ONTAP.
Erro de troca de senha	Verifique credenciais, teste a conetividade SSH e regenere chaves SSH ONTAP. Revise a documentação do switch ou Contate o suporte da NetApp para obter instruções.
Chaves ECDSA não presentes para FIPS	Se o modo FIPS estiver ativado, as chaves ECDSA precisam ser geradas na central antes de tentar novamente.
• Registo pré-existente encontrado*	Remova o arquivo de coleta de logs anterior no switch.

Erro de log de despejo de comutação	Certifique-se de que o usuário do switch tenha permissões de coleta de logs. Consulte os pré-requisitos acima.

Se os detalhes da resolução não funcionarem, entre em Contato com o suporte da NetApp.

Switches de fim de disponibilidade

Término da disponibilidade

Os seguintes switches não estão mais disponíveis para compra, mas ainda são suportados.

- "Cisco Nexus 3232C"
- "Cisco Nexus 3132Q-V"
- "Cisco Nexus 92300YC"
- "NetApp CN1610"

Anúncios de fim de venda e fim de vida útil

- "Anúncio de fim de venda e fim de vida útil do Cisco Nexus 3232C"
- "Anúncio de fim de venda e fim de vida útil para o Cisco Nexus 31108PC-V, 31108TC-V e Nexus 3132Q-V"
- "Anúncio de fim de venda e fim de vida útil do Cisco N9K-C93120TX, N9K-C92300YC"
- "Anúncio de fim de venda e fim de vida útil para os switches Cisco Nexus 5500 Series"
- "Fim da disponibilidade: SKUs de interconexão de cluster NetApp CN1610"

Cisco Nexus 3232C

Comece agora

Fluxo de trabalho de instalação e configuração para switches Cisco Nexus 3232C

Os switches Cisco Nexus 3232C podem ser usados como switches de cluster no seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seu switch Cisco Nexus 3232C.

1 **"Requisitos de configuração"**

Revise os requisitos de configuração para o switch de cluster 3232C.

2 **"Documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 3232C e o cluster ONTAP .

3 **"Requisitos para Smart Call Home"**

Revise os requisitos do recurso Cisco Smart Call Home, usado para monitorar os componentes de hardware e software na sua rede.

4 **"Instale o hardware"**

Instale o hardware do switch.

5 **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches Cisco Nexus 3232C

Para a instalação e manutenção do switch Cisco Nexus 3232C, certifique-se de rever os requisitos de configuração e rede.

Requisitos de configuração

Para configurar o cluster, é necessário o número e o tipo apropriados de cabos e conetores de cabos para os switches. Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para o tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700, a interface e0M utiliza uma porta Ethernet dedicada.

Consulte a "Hardware Universe" para obter informações mais recentes.

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches Cisco Nexus 3232C

Para instalação e manutenção do switch Cisco Nexus 3232C, certifique-se de rever toda a documentação recomendada.

Documentação do switch

Para configurar os switches Cisco Nexus 3232C, você precisa da seguinte documentação na "Suporte para switches Cisco Nexus 3000 Series" página.

Título do documento	Descrição
Guia de Instalação de hardware da Série Nexus 3000	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.

Título do documento	Descrição
Guias de configuração do software de comutador da série Cisco Nexus 3000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
Guia de atualização e downgrade do software NX-os da série Cisco Nexus 3000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
Cisco Nexus 3000 Series NX-os Guia de Referência de comando	Fornece links para as várias referências de comando fornecidas pelo Cisco.
Cisco Nexus 3000 MIBs Referência	Descreve os arquivos MIB (Management Information base) para os switches Nexus 3000.
Nexus 3000 Series NX-os System Message Reference	Descreve as mensagens do sistema para os switches da série Cisco Nexus 3000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de lançamento do Cisco Nexus 3000 Series NX-os (escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 3000 Series.
Informações regulamentares, de conformidade e de segurança para o Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series e Cisco Nexus 2000 Series	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 3000.

Documentação de sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para sua versão do sistema operacional "ONTAP 9" .

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.
Documentação do ONTAP	Fornece informações detalhadas sobre todos os aspetos das versões do ONTAP.

Nome	Descrição
"Hardware Universe"	Fornece informações de compatibilidade e configuração de hardware NetApp.

Kit de trilho e documentação do gabinete

Para instalar um switch Cisco 3232C em um gabinete NetApp, consulte a documentação de hardware a seguir.

Nome	Descrição
"Armário do sistema 42U, guia profundo"	Descreve as FRUs associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição da FRU.
"Instale um switch Cisco Nexus 3232C em um gabinete NetApp"	Descreve como instalar um switch Cisco Nexus 3232C em um gabinete NetApp de quatro colunas.

Requisitos para Smart Call Home

Para usar o Smart Call Home, você deve configurar um switch de rede de cluster para se comunicar por e-mail com o sistema Smart Call Home. Além disso, você pode opcionalmente configurar seu switch de rede de cluster para aproveitar o recurso de suporte Smart Call Home incorporado da Cisco.

O Smart Call Home monitora os componentes de hardware e software na sua rede. Quando ocorre uma configuração crítica do sistema, ele gera uma notificação por e-mail e envia um alerta para todos os destinatários configurados no seu perfil de destino.

Antes de usar o Smart Call Home, esteja ciente dos seguintes requisitos:

- Um servidor de e-mail deve estar no lugar.
- O switch deve ter conetividade IP com o servidor de e-mail.
- É necessário configurar o nome do contacto (contacto do servidor SNMP), o número de telefone e as informações do endereço da rua. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID de CCO deve ser associado a um contrato de serviço Cisco SMARTnet apropriado para a sua empresa.
- O Serviço SMARTnet da Cisco deve estar em vigor para que o dispositivo seja registrado.

O "Site de suporte da Cisco" contém informações sobre os comandos para configurar Smart Call Home.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches Cisco Nexus 3232C

Para instalar e configurar o hardware de um switch de cluster 3232C, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2. "Instale o interrutor"

Instale o switch 3232C.

3. "Instale o interrutor em um gabinete NetApp"

Instale o switch 3232C e o painel de passagem em um gabinete NetApp , conforme necessário.

4. "Revise o cabeamento e a configuração"

Revise o suporte para portas Ethernet NVIDIA .

Folha de cálculo completa de cabeamento do Cisco Nexus 3232C

Se você quiser documentar as plataformas suportadas, baixe um PDF desta página e complete a Planilha de cabeamento.

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

Cada switch pode ser configurado como uma única porta 100GbE, 40GbE ou 4 portas x 10GbE.

Planilha de cabeamento de amostra

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		**Interrutor B do grupo de instrumentos**	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta
1	4x10GbE/4x25GbE ou nó 40/100GbE GbE	1	4x10GbE/4x25GbE ou nó 40/100GbE GbE
2	4x10GbE/4x25GbE ou nó 40/100GbE GbE	2	4x10GbE/4x25GbE ou nó 40/100GbE GbE

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
3	4x10GbE/4x25GbE ou nó 40/100GbE GbE	3	4x10GbE/4x25GbE ou nó 40/100GbE GbE
4	4x10GbE/4x25GbE ou nó 40/100GbE GbE	4	4x10GbE/4x25GbE ou nó 40/100GbE GbE
5	4x10GbE/4x25GbE ou nó 40/100GbE GbE	5	4x10GbE/4x25GbE ou nó 40/100GbE GbE
6	4x10GbE/4x25GbE ou nó 40/100GbE GbE	6	4x10GbE/4x25GbE ou nó 40/100GbE GbE
7	4x10GbE/4x25GbE ou nó 40/100GbE GbE	7	4x10GbE/4x25GbE ou nó 40/100GbE GbE
8	4x10GbE/4x25GbE ou nó 40/100GbE GbE	8	4x10GbE/4x25GbE ou nó 40/100GbE GbE
9	4x10GbE/4x25GbE ou nó 40/100GbE GbE	9	4x10GbE/4x25GbE ou nó 40/100GbE GbE
10	4x10GbE/4x25GbE ou nó 40/100GbE GbE	10	4x10GbE/4x25GbE ou nó 40/100GbE GbE
11	4x10GbE/4x25GbE ou nó 40/100GbE GbE	11	4x10GbE/4x25GbE ou nó 40/100GbE GbE
12	4x10GbE/4x25GbE ou nó 40/100GbE GbE	12	4x10GbE/4x25GbE ou nó 40/100GbE GbE
13	4x10GbE/4x25GbE ou nó 40/100GbE GbE	13	4x10GbE/4x25GbE ou nó 40/100GbE GbE
14	4x10GbE/4x25GbE ou nó 40/100GbE GbE	14	4x10GbE/4x25GbE ou nó 40/100GbE GbE
15	4x10GbE/4x25GbE ou nó 40/100GbE GbE	15	4x10GbE/4x25GbE ou nó 40/100GbE GbE
16	4x10GbE/4x25GbE ou nó 40/100GbE GbE	16	4x10GbE/4x25GbE ou nó 40/100GbE GbE
17	4x10GbE/4x25GbE ou nó 40/100GbE GbE	17	4x10GbE/4x25GbE ou nó 40/100GbE GbE

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
18	4x10GbE/4x25GbE ou nó 40/100GbE GbE	18	4x10GbE/4x25GbE ou nó 40/100GbE GbE
19	Nó 40g/100GbE 19	19	Nó 40g/100GbE 19
20	Nó 40g/100GbE 20	20	Nó 40g/100GbE 20
21	Nó 40g/100GbE 21	21	Nó 40g/100GbE 21
22	Nó 40g/100GbE 22	22	Nó 40g/100GbE 22
23	Nó 40g/100GbE 23	23	Nó 40g/100GbE 23
24	Nó 40g/100GbE 24	24	Nó 40g/100GbE 24
25 a 30	Todos os direitos reservados	25 a 30	Todos os direitos reservados
31	100GbE ISL para a porta 31 do interrutor B.	31	100GbE ISL para mudar A porta 31
32	100GbE ISL para a porta 32 do interrutor B.	32	100GbE ISL para mudar A porta 32

Folha de cálculo de cablagem em branco

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A seção *conexões de cluster suportadas* da "Hardware Universe" define as portas de cluster usadas pela plataforma.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó/porta	Porta do switch	Uso de nó/porta
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 a 30	Todos os direitos reservados	25 a 30	Todos os direitos reservados
31	100GbE ISL para a porta 31 do interrutor B.	31	100GbE ISL para mudar A porta 31

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
32	100GbE ISL para a porta 32 do interrutor B.	32	100GbE ISL para mudar A porta 32

O que vem a seguir

"Instale o interrutor" .

Instalar o switch de cluster 3232C

Siga este procedimento para configurar e configurar o switch Cisco Nexus 3232C.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões NX-os e Reference Configuration File (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- Concluído"fichas de trabalho de cablagem" .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- "Documentação necessária do switch e do ONTAP" .

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o…	Então…
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia *Instalando um switch de cluster Cisco Nexus 3232C e o painel pass-through em um gabinete NetApp* para obter instruções para instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.

O que se segue?

Opcionalmente, você pode"instalar um switch Cisco Nexus 3223C em um gabinete NetApp" . Caso contrário, vá para"Revise o cabeamento e a configuração" .

Instale um switch de cluster Cisco Nexus 3232C em um gabinete NetApp

Dependendo da sua configuração, você pode precisar instalar o switch de cluster Cisco Nexus 3232C e o painel pass-through em um gabinete NetApp com os suportes padrão que estão incluídos no switch.

Antes de começar

- Os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança no "Guia de instalação de hardware do Cisco Nexus 3000 Series".
- Para cada interrutor, os oito parafusos 10-32 ou 12-24 e as porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiros e traseiros do armário.
- Kit de trilho padrão Cisco para instalar o interrutor em um gabinete NetApp.

> Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

   O kit de painel de passagem está disponível na NetApp (código de peça X8784-R6).

   O kit do painel de passagem do NetApp contém o seguinte hardware:

   - Um painel obturador de passagem
   - Quatro parafusos 10-32 x .75
   - Quatro porcas de freio 10-32

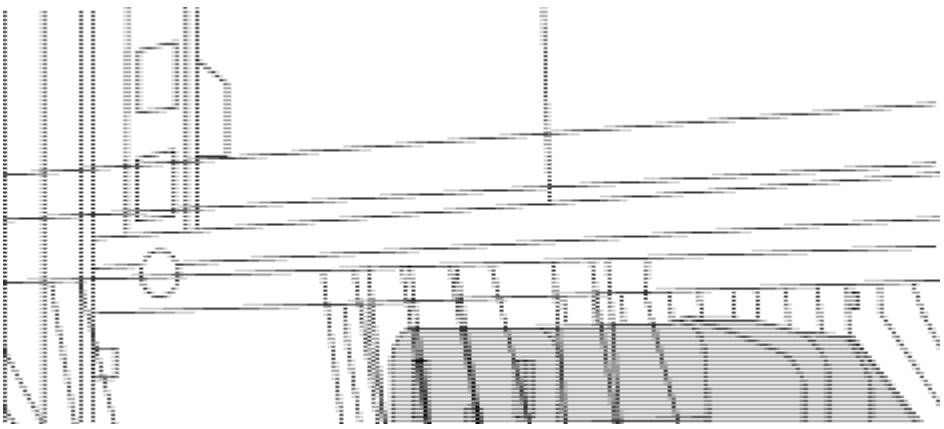
     i. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

     Neste procedimento, o painel obturador será instalado em U40.

     ii. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

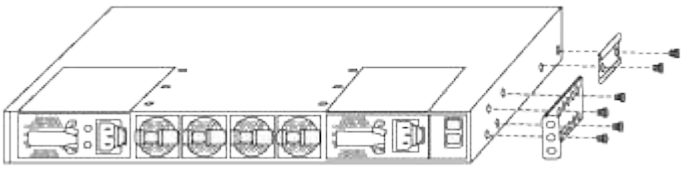
     iii. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

     iv. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.

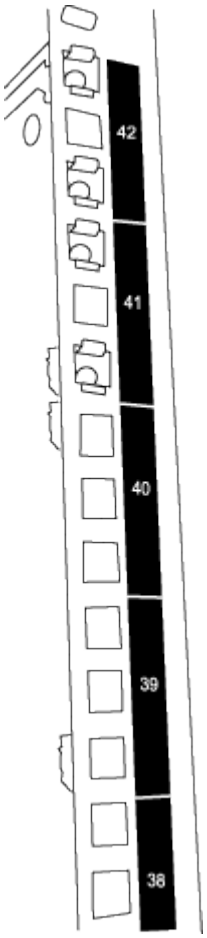


(1) conetor fêmea do cabo de ligação em ponte.

1. Instale os suportes de montagem em rack no chassi do switch Nexus 3232C.
   a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.

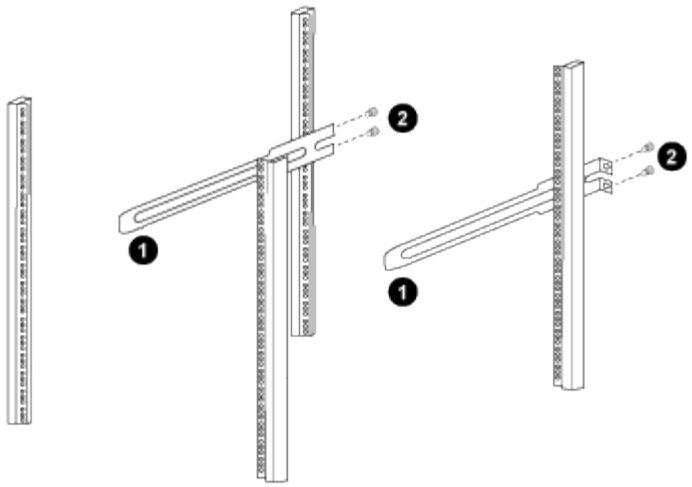


   b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.
   c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.
   d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.
2. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



   Os dois interrutores 3232C serão sempre montados no topo 2U do gabinete RU41 e 42.

3. Instale os trilhos deslizantes no gabinete.
   a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



*(1) ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.*__(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete._

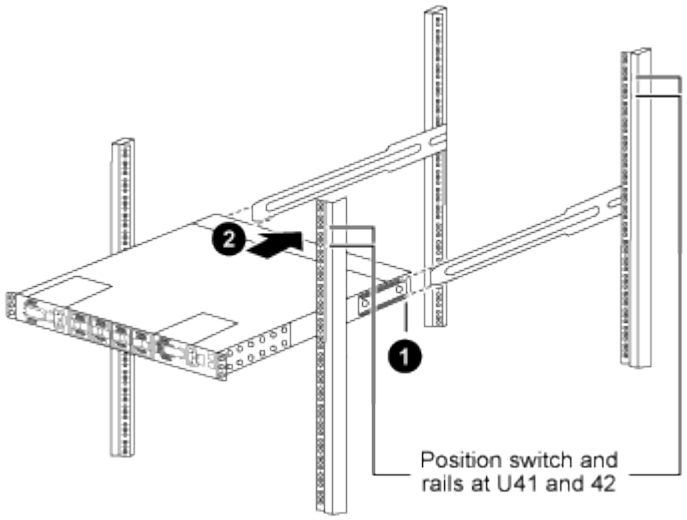
a. Repita o passo 4a para a coluna traseira do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

4. Instale o interrutor no gabinete.

> Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

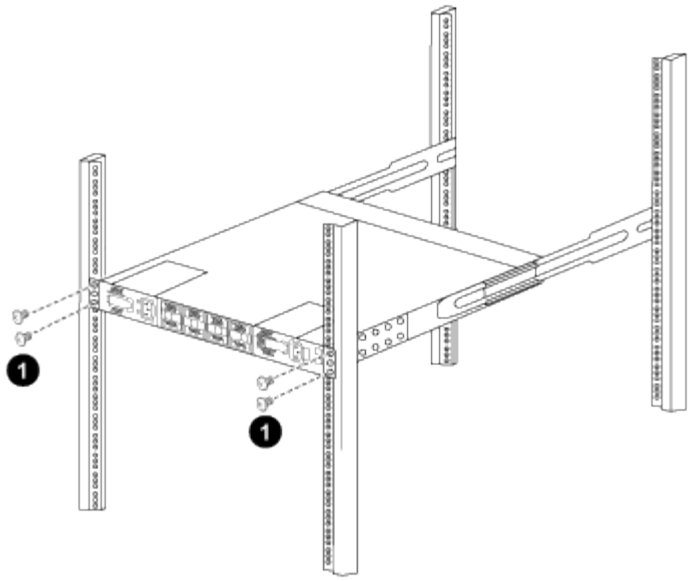
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário manter a frente do segundo interrutor durante o processo de instalação.

5. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
6. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

7. Conete a porta de gerenciamento de cada switch 3232C a um dos switches de gerenciamento (se solicitado) ou conete-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração

Antes de configurar o switch Cisco 3232C, revise as seguintes considerações.

Suporte para portas NVIDIA CX6, CX6-DX e CX7 Ethernet

Se estiver conetando uma porta de switch a um controlador ONTAP usando as portas de NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), é necessário codificar a velocidade da porta do switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Configure o software

Fluxo de trabalho de instalação de software para switches de cluster Cisco Nexus 3232C

Para instalar e configurar o software para um switch Cisco Nexus 3232C e instalar ou atualizar o arquivo de configuração de referência (RCF), siga estas etapas:

1. **"Configure o interrutor"**

Configurar o switch de cluster 3232C.

2. **"Prepare-se para instalar o software NX-os e o RCF"**

O software Cisco NX-OS e os arquivos de configuração de referência (RCFs) devem ser instalados nos switches de cluster Cisco 3232C.

3. **"Instale ou atualize o software NX-os"**

Baixe e instale ou atualize o software NX-OS no switch de cluster Cisco 3232C.

4. **"Instale o RCF"**

Instale o RCF depois de configurar o switch Cisco 3232C pela primeira vez.

5. **"Verifique a configuração do SSH"**

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

6. **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações do switch do cluster 3232C.

Configure o switch do cluster 3232C

Siga este procedimento para configurar e configurar o switch Cisco Nexus 3232C.

Antes de começar

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões de NX-os e arquivo de configuração de referência (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Documentação necessária do switch de rede e gerenciamento de cluster.

  Consulte "Documentação necessária" para obter mais informações.

- Documentação necessária do controlador e documentação do ONTAP.

  "Documentação do NetApp"

- Licenças aplicáveis, informações de rede e configuração e cabos.
- Fichas de trabalho de cablagem concluídas.
- RCFs de rede e de gerenciamento de cluster NetApp aplicáveis, baixados do site de suporte da NetApp em "mysupport.NetApp.com" para os switches que você recebe. Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o seu…	Então…
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia *Instalando um switch de cluster Cisco Nexus 3232C e o painel pass-through em um gabinete NetApp* para obter instruções para instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.
4. Execute uma configuração inicial dos switches de rede do cluster.

   Forneça respostas aplicáveis às seguintes perguntas de configuração inicial ao inicializar o switch pela primeira vez. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Aviso	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com **sim**. A predefinição é não

Aviso	Resposta
Pretende aplicar o padrão de palavra-passe seguro? (sim/não)	Responda com **sim**. O padrão é sim.
Introduza a palavra-passe para admin.	A senha padrão é "'admin'"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Pretende introduzir a caixa de diálogo de configuração básica? (sim/não)	Responda com **sim** na configuração inicial do comutador.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em administradores alternativos. O padrão é **não**.
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com **não**. A predefinição é não
Configurar string de comunidade SNMP de leitura-escrita? (sim/não)	Responda com **não**. A predefinição é não
Introduza o nome do interrutor.	O nome do switch está limitado a 63 carateres alfanuméricos.
Continuar com a configuração de gerenciamento fora da banda (mgmt0)? (sim/não)	Responda com **yes** (o padrão) nesse prompt. No prompt mgmt0 IPv4 address:, insira seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com **sim**. No endereço IPv4 do prompt default-gateway:, digite seu default_gateway.
Configurar opções IP avançadas? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço telnet? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço SSH? (sim/não)	Responda com **sim**. O padrão é sim. O SSH é recomendado ao usar o Ethernet Switch Health Monitor (CSHM) para seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Introduza o tipo de chave SSH que pretende gerar (dsa/rsa/rsa1).	O padrão é **rsa**.
Introduza o número de bits de chave (1024-2048).	Introduza o número de bits de chave de 1024-2048.

Aviso	Resposta
Configurar o servidor NTP? (sim/não)	Responda com **não**. A predefinição é não
Configurar a camada de interface padrão (L3/L2):	Responda com **L2**. A predefinição é L2.
Configurar o estado predefinido da interface da porta do switch (Shut/noshut):	Responda com **noshut**. O padrão é noshut.
Configurar o perfil do sistema CoPP (strict/moderate/lenient/dense):	Responda com **strict**. O padrão é rigoroso.
Pretende editar a configuração? (sim/não)	Você deve ver a nova configuração neste momento. Reveja e faça as alterações necessárias à configuração que acabou de introduzir. Responda com **no** no prompt se você estiver satisfeito com a configuração. Responda com **yes** se quiser editar as configurações.
Utilizar esta configuração e guardá-la? (sim/não)	Responda com **yes** para salvar a configuração. Isto atualiza automaticamente as imagens do Kickstart e do sistema. Se você não salvar a configuração nesta fase, nenhuma das alterações entrará em vigor na próxima vez que você reiniciar o switch.

5. Verifique as opções de configuração que você fez no visor que aparece no final da configuração e certifique-se de salvar a configuração.
6. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software suportada pelo NetApp para os switches a partir da "Transferência do software Cisco" página.

O que se segue?

"Prepare-se para instalar o NX-os e o RCF".

Preparar para instalar o software NX-os e o ficheiro de configuração de referência (RCF)

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento usam dois nós. Esses nós usam duas portas de interconexão de cluster 10GbE `e0a` e `e0b`.

Consulte "Hardware Universe"para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Nomenclatura de switch e nó

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `cluster1-01` e `cluster1-02`.
- Os nomes de LIF do cluster são `cluster1-01_clus1` e `cluster1-01_clus2` para cluster1-01 e `cluster1-02_clus1` e `cluster1-02_clus2` para cluster1-02.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:
   `system node autosupport invoke -node * -type all -message MAINT=x h`

   onde *x* é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   `set -privilege advanced`

   (`*>`É apresentado o aviso avançado).

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster:

   `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N3K-
C3232C
            e0b    cs2                       Eth1/2            N3K-
C3232C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N3K-
C3232C
            e0b    cs2                       Eth1/1            N3K-
C3232C

4 entries were displayed.
```

4. Verifique o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede:

      `network port show –ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

a. Exibir informações sobre os LIFs:
`network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none
.
.
cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o `auto-revert` comando está ativado em todas as LIFs do cluster:
`network interface show -vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

O que se segue?

"Instale o software NX-os" .

Instale o software NX-os

Você pode usar este procedimento para instalar o software NX-os no switch de cluster Nexus 3232C.

Rever os requisitos

Antes de começar

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- "Página do switch Ethernet Cisco". Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.
- "Switches Cisco Nexus 3000 Series". Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Certifique-se de que conclui o procedimento em "Prepare-se para instalar o NX-os e o RCF"e, em seguida, siga os passos abaixo.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch pode alcançar o servidor no endereço IP 172.19.2.1:

   ```
   cs2# ping 172.19.2.1
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
----------
cs1                         cluster-network    10.233.205.90    N3K-
C3232C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N3K-
C3232C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Copie o software NX-os e as imagens EPLD para o switch Nexus 3232C.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.4.img  /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
  NXOS compile time:  12/22/2019 2:00:00 [12/22/2019 14:00:37]

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGD

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

8. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS


Compatibility check is done:
Module  bootable          Impact              Install-type  Reason
------- ----------------- ------------------- -------------
----------
     1     Yes            Disruptive          Reset         Default
upgrade is not hitless


Images will be upgraded according to following table:
Module       Image       Running-Version(pri:alt)
New-Version          Upg-Required
------------ ----------- ----------------------------------------
-------------------- ------------
     1       nxos        9.3(3)
9.3(4)               yes
     1       bios        v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)   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.
cs2#
```

9. Verifique a nova versão do software NX-os depois que o switch reiniciar:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  NXOS: version 9.3(4)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
 cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
  Reason: Reset due to upgrade
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

10. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                            0x12
IO   FPGA                            0x11

cs2# install epld bootflash:n9000-epld.9.3.4.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                0x12         0x12         No
     1   SUP   IO FPGA                0x11         0x12         Yes
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

Module 1 EPLD upgrade is successful.
cs2#
```

11. Se estiver a atualizar para a versão NX-os 9,3(11), tem de atualizar a imagem EPLD `golden` e reiniciar a central novamente. Caso contrário, vá para o passo 12.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/epld-rn/nxos_n9K_epldRN_9311.html["Notas de versão de atualização do EPLD, versão 9,3(11)"^]Consulte para obter mais detalhes.

Mostrar exemplo

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module        Type         Upgradable     Impact      Reason
------  -----------------  -------------  ----------
-----------------
     1        SUP          Yes            Disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
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 : MI FPGA [Programming] : 100.00% (     64 of      64 sect)
Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sect)
Module 1 EPLD upgrade is successful.
Module        Type          Upgrade-Result
------  ------------------  --------------
     1         SUP          Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#
```

12. Após a reinicialização do switch, faça login para verificar se a nova versão do EPLD foi carregada com sucesso.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x12
IO   FPGA                             0x12
```

13. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -role cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
----------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ---------------
----------
cs1                         cluster-network    10.233.205.90    N3K-
C3232C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N3K-
```

```
C3232C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

14. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

15. Repita os passos 6 a 14 no interrutor CS1.
16. Ative a reversão automática nos LIFs do cluster.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

17. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que se segue?

"Instale o arquivo de configuração RCF".

Instalar ou atualizar o ficheiro de configuração de referência (RCF)

Siga este procedimento para instalar o RCF depois de configurar o switch Nexus 3232C pela primeira vez.

Você também pode usar este procedimento para atualizar sua versão RCF. Consulte o artigo da base de

dados de Conhecimento "Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para obter mais informações ao atualizar o RCF.

Rever os requisitos

Antes de começar

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O ficheiro de configuração de referência atual (RCF).
- Uma ligação de consola ao interrutor, necessária ao instalar o RCF.
- "Página do switch Ethernet Cisco" Consulte a tabela de compatibilidade do switch para as versões ONTAP e RCF suportadas. Note que pode haver dependências de comando entre a sintaxe de comando no RCF e aquela encontrada em versões do NX-os.
- "Switches Cisco Nexus 3000 Series". Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

Instale o ficheiro

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `cluster1-01` `cluster1-02` , , `cluster1-03` `cluster1-04` e .
- Os nomes de LIF do cluster são `cluster1-01_clus1`, `cluster1-01_clus2` `cluster1-02_clus1` , `cluster1-02_clus2` , `cluster1-03_clus1`, , , `cluster1-03_clus2`, `cluster1-04_clus1`, e `cluster1-04_clus2`.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Certifique-se de que conclui o procedimento em "Prepare-se para instalar o NX-os e o RCF"e, em seguida, siga os passos abaixo.

Passos

1. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      `network port show –role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

`system cluster-switch show -is-monitoring-enabled-operational true`

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.233.205.92
NX3232C
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.93
NX3232C
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Desative a reversão automática nos LIFs do cluster.

Mostrar exemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

4. No switch de cluster CS2, encerre as portas conetadas às portas de cluster dos nós.

Mostrar exemplo

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

5. Verifique se as portas de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

   `network interface show -role cluster`

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
8 entries were displayed.
cluster1::*>
```

6. Verifique se o cluster está em bom estado:

   `cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

7. Se você ainda não fez isso, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

   `show running-config`

8. Registre quaisquer adições personalizadas entre o atual `running-config` e o arquivo RCF em uso.
9. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

   Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conectado à porta serial do console do switch para configurá-lo novamente.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg

cs2# show run | section "hostname" >> bootflash:write_erase.cfg

cs2# show run | i "username admin password" >> bootflash:write_erase.cfg

cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

10. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
bootflash:write_erase.cfg

cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

    Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

11. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

    `show file bootflash:write_erase.cfg`

12. Emitir o `write erase` comando para apagar a configuração salva atual:

```
cs2# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

13. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

14. Execute uma reinicialização do switch:

```
cs2# reload

This command will reboot the system. (y/n)? [n] y
```

15. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 3000 Series NX-os" guias.

Mostrar exemplo

Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server......Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

16. Aplique o RCF baixado anteriormente ao flash de inicialização.

Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 3000 Series NX-os" guias.

Mostrar exemplo

Este exemplo mostra o arquivo RCF `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` sendo instalado no switch CS2:

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

17. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir as instruções em **Notas importantes** para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs2# show banner motd

**********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Cisco Nexus 3232C
* Filename : Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : Oct-20-2020
* Version  : v1.6
*
* Port Usage : Breakout configuration
* Ports  1- 3: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4
* Ports  4- 6: Breakout mode (4x25GbE) Intra-Cluster/HA Ports, int
e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports  7-30: 40/100GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* Ports 33-34: 10GbE Intra-Cluster 10GbE Ports, int e1/33-34
*
* IMPORTANT NOTES
* - Load Nexus_3232C_RCF_v1.6-Cluster-HA.txt for non breakout config
*
* - This RCF utilizes QoS and requires TCAM re-configuration,
requiring RCF
*   to be loaded twice with the Cluster Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class IPv4
ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
```

```
*
*    (4) Save running-configuration again
**********************************************************************
**********
```

Ao aplicar o RCF pela primeira vez, a mensagem **ERROR: Failed to write VSH commands** é esperada e pode ser ignorada.

18. Verifique se o arquivo RCF é a versão mais recente correta:

    `show running-config`

    Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

    - O banner RCF
    - As configurações de nó e porta
    - Personalizações

      A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

19. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
20. Depois de verificar se as versões do RCF e as configurações do switch estão corretas, copie o arquivo running-config para o arquivo startup-config.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 3000 Series NX-os" nos guias.

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

21. Interrutor de reinicialização CS2. Você pode ignorar os eventos "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
cs2# reload
This command will reboot the system. (y/n)?  [n] y
```

22. Aplique o mesmo RCF e salve a configuração em execução pela segunda vez.

Mostrar exemplo

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

23. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas e0d estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -role cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch CS2, uma vez que LIFs não são homed em e0d).

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7
N3K-C3232C
            e0d    cs2                       Ethernet1/7
N3K-C3232C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8
N3K-C3232C
            e0d    cs2                       Ethernet1/8
N3K-C3232C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1
N3K-C3232C
            e0b    cs2                       Ethernet1/1/1
N3K-C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2
N3K-C3232C
            e0b    cs2                       Ethernet1/1/2
N3K-C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90
N3K-C3232C
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
```

```
N3K-C3232C
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF previamente carregada no switch

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001.
Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092.
Inconsistent local vlan.
```

Pode levar até 5 minutos para que os nós de cluster relatem como íntegros.

24. No switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

Mostrar exemplo

O exemplo a seguir usa a saída de exemplo de interface do passo 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

25. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch CS2. Isso pode levar alguns segundos.

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

26. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

27. Repita os passos 7 a 23 no switch cs1.
28. Ative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert true
```

29. Verifique se as portas do switch conetadas às portas do cluster estão ativadas.

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

30. Verifique se o ISL entre CS1 e CS2 está funcional:

```
show port-channel summary
```

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
cs1#
```

31. Verifique se os LIFs do cluster reverteram para sua porta inicial:

    `network interface show -role cluster`

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFS de cluster não retornou às suas portas iniciais, reverta-as manualmente: `network interface revert -vserver vserver_name -lif lif_name`

32. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------- -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

33. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none
.
.
cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
.
.
cluster1-03
.
.
.
.
cluster1-04
.
.
.
.
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

O que se segue?

"Verifique a configuração do SSH".

Verifique a configuração da SSH

Se você estiver usando os recursos CSHM (Ethernet Switch Health Monitor) e coleta de logs, verifique se as chaves SSH e SSH estão habilitadas nos switches de cluster.

Passos

1. Verifique se o SSH está ativado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verifique se as chaves SSH estão ativadas:

```
show ssh key
```

Mostrar exemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Ao ativar o FIPS, você deve alterar o número de bits para 256 na central usando o comando `ssh key ecdsa 256 force`. "Configurar a segurança da rede usando o FIPS"Consulte para obter mais detalhes.

O que se segue?

"Configurar o monitoramento de integridade do switch".

Redefinir o switch do cluster 3232C para os padrões de fábrica

Para redefinir o switch de cluster 3232C para os padrões de fábrica, você deve apagar as configurações do switch 3232C.

Sobre esta tarefa

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

Passos

1. Apagar a configuração existente:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Recarregue o software do switch:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   O sistema é reinicializado e entra no assistente de configuração. Durante a inicialização, se você receber o prompt “Abortar provisionamento automático e continuar com a configuração normal? (sim/não)[n]”, você deve responder **sim** para prosseguir.

Migrar switches

Migração de switch de CN1610 GbE

Migre de CN1610 switches para o fluxo de trabalho dos switches Nexus 3232C

Siga estas etapas do fluxo de trabalho para migrar seus switches CN1610 para switches Cisco Nexus 3232C.

1. **"Requisitos de migração"**

   Revise as informações de exemplo do switch para o processo de migração.

2. **"Prepare-se para a migração"**

Prepare seus switches CN1610 para migração para os switches Nexus 3232C.

3 **"Substitua o interrutor do cluster CL2"**

Substitua o switch de cluster CL2 pelo novo switch Nexus 3232C C2.

4 **"Substitua o interrutor do cluster CL1"**

Substitua o switch de cluster CL1 pelo novo switch Nexus 3232C C1.

5 **"Conclua a migração"**

Conclua a migração para os novos switches Nexus 3232C.

Requisitos de migração

Os switches Cisco Nexus 3232C podem ser usados como switches de cluster no seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

> O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Se necessário, consulte o seguinte para obter mais informações:

- "NetApp CN1601 e CN1610"
- "Switches Ethernet Cisco"
- "Hardware Universe"

Requisitos de migração de CN1610

Os switches do cluster suportam as seguintes conexões de nós:

- NetApp CN1610: Portas de 0/1 a 0/12 (10 GbE)
- Cisco Nexus 3232C: Portas E1/1-30 (40 ou 100 GbE ou 4x10GbE)

Os interrutores do grupo de instrumentos utilizam as seguintes portas ISL (Inter-switch link).

- NetApp CN1610: Portas de 0/13 a 0/16 (10 GbE)
- Cisco Nexus 3232CX: Portas 1/31-32 (100GbE)

> Você deve usar cabos de ligação 4x10G no switch de cluster Cisco Nexus 3232C.

A tabela a seguir mostra as conexões de cabeamento que são necessárias em cada etapa durante a transição dos switches NetApp CN1610 para os switches de cluster Cisco Nexus 3232C:

Fase	Descrição	Cabos necessários
Inicial	CN1610 GbE para CN1610 GbE (SFP)	4 cabos de conexão direta de fibra ótica ou cobre SFP
Transição	CN1610 GbE para 3232C GbE (QSFP para SFP)	Cabos de fibra ótica ou cobre de 1 QSFP e 4GbE SFP
Final	3232C GbE a 3232C GbE (QSFP para QSFP)	Cabos de conexão direta de fibra ótica de 2 QSFP ou cobre

Você deve ter baixado os arquivos de configuração de referência aplicáveis (RCFs). O número de portas 10 GbE e 40/100 GbE são definidos nos RCFs disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .

As versões ONTAP e NX-OS suportadas neste procedimento estão listadas em"Switches Ethernet Cisco" .

As versões ONTAP e FASTPATH suportadas neste procedimento estão listadas em"Switches NetApp CN1601 e CN1610" .

Sobre os exemplos usados

Os exemplos no procedimento de migração usam quatro nós:

- Dois nós usam quatro portas de interconexão de cluster de 10 GbE: **e0a**, **e0b**, **e0c** e **e0d**.
- Os outros dois nós usam dois cabos de fibra de interconexão de cluster de 40 GbE: **e4a** e **e4e**.

  "*Hardware Universe*"O tem informações sobre os cabos de fibra de cluster para suas plataformas.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nós são **n1**, **n2**, **n3** e **n4**.
- As saídas de comando podem variar dependendo de diferentes versões do software ONTAP.
- Os CN1610 interrutores a substituir são **CL1** e **CL2**.
- Os switches Nexus 3232C para substituir os switches CN1610 são **C1** e **C2**.
- **n1_clus1** é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- **n1_clus2** é o primeiro LIF de cluster conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus3** é o segundo LIF que está conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus4** é o segundo LIF que está conetado ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- O número de portas de 10 GbE e 40/100 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .

O que se segue?

"Prepare-se para a migração".

Siga estes passos para preparar a migração de switch CN1610 para um switch Cisco Nexus 3232C.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   ⓘ A mensagem notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   ```
   network device-discovery show
   ```

   Mostrar exemplo

   O exemplo a seguir mostra quantas interfaces de interconexão de cluster foram configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   cluster::> network device-discovery show

          Local  Discovered
   Node   Port   Device       Interface   Platform
   ------ ------ ------------ ----------- ----------
   n1     /cdp
           e0a   CL1          0/1         CN1610
           e0b   CL2          0/1         CN1610
           e0c   CL2          0/2         CN1610
           e0d   CL1          0/2         CN1610
   n2     /cdp
           e0a   CL1          0/3         CN1610
           e0b   CL2          0/3         CN1610
           e0c   CL2          0/4         CN1610
           e0d   CL1          0/4         CN1610

   8 entries were displayed.
   ```

3. Determine o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede do cluster:

      ```
      network port show -role cluster
      ```

Mostrar exemplo

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1
                 Broadcast               Speed (Mbps) Health Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster    cluster    up    9000  auto/10000     -
e0b   cluster    cluster    up    9000  auto/10000     -
e0c   cluster    cluster    up    9000  auto/10000     -        -
e0d   cluster    cluster    up    9000  auto/10000     -        -
Node: n2
                 Broadcast               Speed (Mbps) Health Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster    cluster    up    9000  auto/10000     -
e0b   cluster    cluster    up    9000  auto/10000     -
e0c   cluster    cluster    up    9000  auto/10000     -
e0d   cluster    cluster    up    9000  auto/10000     -

8 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true

 8 entries were displayed.
```

c. Exibir informações sobre os switches de cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo a seguir exibe os switches de cluster que são conhecidos pelo cluster junto com seus endereços IP de gerenciamento:

```
cluster::> system cluster-switch show
Switch                        Type              Address       Model
----------------------------- ----------------- ------------
--------
CL1                           cluster-network   10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP
CL2                           cluster-network   10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

2   entries displayed.
```

4. Verifique se o RCF e a imagem apropriados estão instalados nos novos switches 3232C conforme necessário para seus requisitos e faça as personalizações essenciais do site.

   Você deve preparar ambos os interrutores neste momento. Se necessitar de atualizar o RCF e a imagem, tem de concluir o seguinte procedimento:

   a. Ver"Switches Ethernet Cisco" no site de suporte da NetApp .
   b. Observe o switch e as versões de software necessárias na tabela nessa página.
   c. Baixe a versão apropriada do RCF.
   d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
   e. Baixe a versão apropriada do software de imagem em"Download do arquivo de configuração de referência do comutador de rede de gerenciamento e cluster Cisco" .

5. Migre os LIFs associados ao segundo switch CN1610 que você planeja substituir:

   `network interface migrate -vserver` *`vserver-name`* `-lif` *`lif-name`* `-source-node` *`source-node-name`* `destination-node` *`destination-node-name`* `-destination-port` *`destination-port-name`*

Mostrar exemplo

Você deve migrar cada LIF individualmente, conforme mostrado no exemplo a seguir:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2
-source-node n1
-destination-node  n1  -destination-port  e0a
cluster::*> network interface migrate -vserver cluster -lif n1_clus3
-source-node n1
-destination-node  n1  -destination-port  e0d
cluster::*> network interface migrate -vserver cluster -lif n2_clus2
-source-node n2
-destination-node  n2  -destination-port  e0a
cluster::*> network interface migrate -vserver cluster -lif n2_clus3
-source-node n2
-destination-node  n2  -destination-port  e0d
```

6. Verifique a integridade do cluster:

   `network interface show -role cluster`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network         Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask    Node     Port
Home
-------- ---------- ----------- --------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24    n1        e0a
true
         n1_clus2   up/up       10.10.0.2/24    n1        e0a
false
         n1_clus3   up/up       10.10.0.3/24    n1        e0d
false
         n1_clus4   up/up       10.10.0.4/24    n1        e0d
true
         n2_clus1   up/up       10.10.0.5/24    n2        e0a
true
         n2_clus2   up/up       10.10.0.6/24    n2        e0a
false
         n2_clus3   up/up       10.10.0.7/24    n2        e0d
false
         n2_clus4   up/up       10.10.0.8/24    n2        e0d
true

8 entries were displayed.
```

O que se segue?

"Substitua o interrutor CN1610 CL2 pelo interrutor 3232C C2".

Substitua o interrutor CN1610 CL2 pelo interrutor 3232C C2

Siga estas etapas para substituir o switch CN1610 (CL2) por um switch Nexus 3232C (C2).

Passos

1. Encerre as portas de interconexão de cluster que estão fisicamente conetadas ao switch CL2:

```
network port modify -node node-name -port port-name -up-admin false
```

Mostrar exemplo

O exemplo a seguir mostra as quatro portas de interconexão de cluster que estão sendo encerradas para o nó n1 e o nó n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. encerre as portas ISL 13 a 16 no interrutor CN1610 ativo CL1 usando o comando apropriado.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL 13 a 16 estão sendo desligadas no switch CN1610 CL1:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16
(CL1)(Interface 0/13-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

2. Construa um ISL temporário entre CL1 e C2:

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra um ISL temporário sendo construído entre CL1 (portas 13-16) e C2 (portas E1/24/1-4) usando o comando Cisco `switchport mode trunk`:

   ```
   C2# configure
   C2(config)# interface port-channel 2
   C2(config-if)# switchport mode trunk
   C2(config-if)# spanning-tree port type network
   C2(config-if)# mtu 9216
   C2(config-if)# interface breakout module 1 port 24 map 10g-4x
   C2(config)# interface e1/24/1-4
   C2(config-if-range)# switchport mode trunk
   C2(config-if-range)# mtu 9216
   C2(config-if-range)# channel-group 2 mode active
   C2(config-if-range)# exit
   C2(config-if)# exit
   ```

3. Remova os cabos que estão conetados ao switch CN1610 CL2 em todos os nós.

   Com o cabeamento compatível, você deve reconetar as portas desconetadas em todos os nós ao switch Nexus 3232C C2.

4. Remova quatro cabos ISL das portas 13 a 16 no interrutor CN1610 CL1.

   Você deve conetar o Cisco QSFP28 apropriado aos cabos de conexão SFP 1/24 no novo switch Cisco 3232C C2 às portas 13 a 16 no switch CN1610 existente CL1.

Ao reconetar quaisquer cabos ao novo switch Cisco 3232C, os cabos usados devem ser de fibra ótica ou cabos Cisco twinax.

5. Torne o ISL dinâmico configurando a interface ISL 3/1 no interrutor CN1610 ativo para desativar o modo estático.

   Esta configuração corresponde à configuração ISL no interrutor 3232C C2 quando os ISLs são apresentados em ambos os interrutores.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra a interface ISL 3/1 sendo configurada para tornar o ISL dinâmico:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 3/1
   (CL1)(Interface 3/1)# no port-channel static
   (CL1)(Interface 3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

6. Abra ISLs 13 a 16 no interrutor CN1610 ativo CL1.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra que as portas ISL 13 a 16 estão sendo criadas na interface de canal de porta 3/1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 0/13-0/16,3/1
   (CL1)(Interface 0/13-0/16,3/1)# no shutdown
   (CL1)(Interface 0/13-0/16,3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

7. Verifique se as ISLs estão `up` no interrutor CN1610 CL1.

   O "Estado da ligação" deve ser `Up`, "tipo" deve ser `Dynamic`, e a coluna "porta ativa" deve ser `True` para as portas 0/13 a 0/16.

Mostrar exemplo

O exemplo a seguir mostra os ISLs que estão sendo verificados como `up` no switch CN1610 CL1:

```
(CL1)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port         Port
Ports  Timeout       Speed        Active
------ ------------- ----------   -------
0/13   actor/long    10 Gb Full   True
       partner/long
0/14   actor/long    10 Gb Full   True
       partner/long
0/15   actor/long    10 Gb Full   True
       partner/long
0/16   actor/long    10 Gb Full   True
       partner/long
```

8. Verifique se as ISLs estão `up` no interrutor 3232C C2:

   `show port-channel summary`

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   As portas eth1/24/1 a eth1/24/4 devem indicar `(P)`, o que significa que todas as quatro portas ISL estão no canal da porta. eth1/31 e eth1/32 devem indicar `(D)` uma vez que não estão ligados.

Mostrar exemplo

O exemplo a seguir mostra os ISLs que estão sendo verificados como `up` no switch 3232C C2:

```
C2# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
----------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
----------
1       Po1(SU)     Eth      LACP      Eth1/31(D)   Eth1/32(D)
2       Po2(SU)     Eth      LACP      Eth1/24/1(P) Eth1/24/2(P)
Eth1/24/3(P)
                                       Eth1/24/4(P)
```

9. Abra todas as portas de interconexão de cluster que estão conetadas ao switch 3232C C2 em todos os nós:

   `network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin true`

Mostrar exemplo

O exemplo a seguir mostra como abrir as portas de interconexão de cluster conetadas ao switch 3232C C2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

10. Reverter todas as LIFs de interconexão de cluster migradas que estão conetadas ao C2 em todos os nós:

    `network interface revert -vserver cluster -lif` *`lif-name`*

Mostrar exemplo

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
```

11. Verifique se todas as portas de interconexão de cluster são revertidas para suas portas iniciais:

`network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra que os LIFs no clus2 são revertidos para suas portas home; os LIFs são revertidos com sucesso se as portas na coluna "porta atual" tiverem um status de `true` na coluna "está Home". Se o valor "está em Casa" for `false`, então o LIF não será revertido.

```
cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true

8 entries were displayed.
```

12. Verifique se todas as portas do cluster estão conetadas:

`network port show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra a saída verificando que todas as interconexões de cluster são `up`:

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1
                Broadcast                Speed (Mbps) Health   Ignore
Port  IPspace   Domain      Link  MTU    Admin/Open   Status   Health
Status
----- --------- ----------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster     up    9000  auto/10000     -
e0b   cluster   cluster     up    9000  auto/10000     -
e0c   cluster   cluster     up    9000  auto/10000     -        -
e0d   cluster   cluster     up    9000  auto/10000     -        -
Node: n2

                Broadcast                Speed (Mbps) Health   Ignore
Port  IPspace   Domain      Link  MTU    Admin/Open   Status   Health
Status
----- --------- ----------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster     up    9000  auto/10000     -
e0b   cluster   cluster     up    9000  auto/10000     -
e0c   cluster   cluster     up    9000  auto/10000     -
e0d   cluster   cluster     up    9000  auto/10000     -

8 entries were displayed.
```

13. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. migre os LIFs associados ao primeiro switch CN1610 CL1:

   `network interface migrate -vserver cluster -lif` *`lif-name`* `-source-node` *`node-name`*

Mostrar exemplo

É necessário migrar cada LIF de cluster individualmente para as portas de cluster apropriadas hospedadas no switch de cluster C2, conforme mostrado no exemplo a seguir:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n1_clus4
-source-node n1
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n2_clus4
-source-node n2
-destination-node n2 -destination-port e0c
```

O que se segue?

"Substitua o interrutor CN1610 CL1 pelo interrutor 3232C C1".

Substitua o interrutor CN1610 CL1 pelo interrutor 3232C C1

Siga estas etapas para substituir o switch CN1610 (CL1) por um switch Nexus 3232C (C1).

Passos

1. Verifique o status do cluster:

```
network interface show -role cluster
```

Mostrar exemplo

O exemplo a seguir mostra que as LIFs de cluster necessárias foram migradas para as portas de cluster apropriadas hospedadas no switch de cluster C2:

```
cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0b
false
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0c
false
         n2_clus1   up/up       10.10.0.5/24   n2       e0b
false
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0c
false

8 entries were displayed.
```

2. Encerre as portas de nós que estão conetadas ao CL1 em todos os nós:

`network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin false`

Mostrar exemplo

O exemplo a seguir mostra portas específicas sendo fechadas nos nós n1 e n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

3. Desligue as portas ISL 24, 31 e 32 no interrutor 3232C ativo C2.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra que ISLs 24, 31 e 32 estão sendo encerrados no interrutor 3232C ativo C2:

   ```
   C2# configure
   C2(config)# interface ethernet 1/24/1-4
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# interface ethernet 1/31-32
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# exit
   C2#
   ```

4. Remova os cabos que estão conetados ao switch CN1610 CL1 em todos os nós.

   Usando o cabeamento apropriado, você deve reconetar as portas desconetadas em todos os nós ao switch Nexus 3232C C1.

5. Remova os cabos QSFP28 da porta E1/24 do Nexus 3232C C2.

   É necessário conetar as portas E1/31 e E1/32 no C1 às portas E1/31 e E1/32 no C2 usando fibra ótica Cisco QSFP28 suportada ou cabos de conexão direta.

6. Restaure a configuração na porta 24 e remova o canal de porta temporário 2 no C2:

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra o `running-configuration` arquivo que está sendo copiado para o `startup-configuration` arquivo:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 100GbE/40GbE Node Port
C2(config-if)# spanning-tree port type edge
Edge port type (portfast) should only be enabled on ports connected
to a single
host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet 1/24 but
will only
have effect when the interface is in a non-trunking mode.

C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

7. Abra as portas ISL 31 e 32 no C2, o interrutor 3232C ativo.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra ISLs 31 e 32 sendo trazidos para o interrutor 3232C C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

8. Verifique se as conexões ISL estão `up` no interrutor 3232C C2.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra as conexões ISL sendo verificadas. As portas eth1/31 e eth1/32 indicam `(P)`, o que significa que ambas as portas ISL estão `up` no canal de porta:

```
C1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
----------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
---------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)

C2# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
----------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
----------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
```

9. Abra todas as portas de interconexão de cluster conetadas ao novo switch 3232C C1 em todos os nós:

   `network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin true`

Mostrar exemplo

O exemplo a seguir mostra todas as portas de interconexão de cluster conetadas ao novo switch 3232C C1 sendo criado:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

10. Verifique o status da porta do nó do cluster:

```
network port show -role cluster
```

Mostrar exemplo

O exemplo a seguir mostra a saída que verifica se as portas de interconexão de cluster nos nós n1 e n2 no novo switch 3232C C1 são `up`:

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

Node: n2
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -
e0d   cluster   cluster    up    9000  auto/10000     -

8 entries were displayed.
```

O que se segue?

"Conclua a migração".

Conclua sua migração de CN1610 switches para 3232C switches

Conclua as etapas a seguir para finalizar a migração de switches CN1610 para os switches Nexus 3232C.

Passos

1. Reverter todas as LIFs de interconexão de cluster migradas originalmente conetadas ao C1 em todos os nós:

   `network interface revert -server cluster -lif lif-name`

Mostrar exemplo

Você deve migrar cada LIF individualmente, conforme mostrado no exemplo a seguir:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n1_clus4
cluster::*> network interface revert -vserver cluster -lif n2_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus4
```

2. Verifique se a interface está agora em casa:

   `network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra o status das interfaces de interconexão de cluster é `up` e "é Início" para os nós n1 e n2:

```
cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true

8 entries were displayed.
```

3. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
3 paths up, 0 paths down (udp check)
```

1. expanda o cluster adicionando nós aos switches de cluster Nexus 3232C.
2. Exiba as informações sobre os dispositivos em sua configuração:
   - `network device-discovery show`

- network port show -role cluster
- network interface show -role cluster
- system cluster-switch show

Mostrar exemplo

Os exemplos a seguir mostram os nós n3 e n4 com portas de cluster de 40 GbE conetadas às portas E1/7 e E1/8, respetivamente, em ambos os switches de cluster Nexus 3232C. Ambos os nós são Unidos ao cluster. As portas de interconexão de cluster de 40 GbE usadas são e4a e e4e.

```
cluster::*> network device-discovery show

       Local  Discovered
Node   Port   Device       Interface       Platform
------ ------ ------------ --------------- -------------
n1     /cdp
        e0a   C1           Ethernet1/1/1   N3K-C3232C
        e0b   C2           Ethernet1/1/1   N3K-C3232C
        e0c   C2           Ethernet1/1/2   N3K-C3232C
        e0d   C1           Ethernet1/1/2   N3K-C3232C
n2     /cdp
        e0a   C1           Ethernet1/1/3   N3K-C3232C
        e0b   C2           Ethernet1/1/3   N3K-C3232C
        e0c   C2           Ethernet1/1/4   N3K-C3232C
        e0d   C1           Ethernet1/1/4   N3K-C3232C

n3     /cdp
        e4a   C1           Ethernet1/7     N3K-C3232C
        e4e   C2           Ethernet1/7     N3K-C3232C

n4     /cdp
        e4a   C1           Ethernet1/8     N3K-C3232C
        e4e   C2           Ethernet1/8     N3K-C3232C

12 entries were displayed.
cluster::*> network port show -role cluster
(network port show)

Node: n1
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -
```

```
Node: n2
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -
e0d   cluster   cluster    up    9000  auto/10000     -        -

Node: n3
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -
e4e   cluster   cluster    up    9000  auto/40000     -        -

Node: n4
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -
e4e   cluster   cluster    up    9000  auto/40000     -

12 entries were displayed.

cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
```

```
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true
         n3_clus1   up/up       10.10.0.9/24   n3       e4a
true
         n3_clus2   up/up       10.10.0.10/24  n3       e4e
true
         n4_clus1   up/up       10.10.0.11/24  n4       e4a
true
         n4_clus2   up/up       10.10.0.12/24  n4       e4e
true

12 entries were displayed.

cluster::> system cluster-switch show

Switch                      Type              Address       Model
--------------------------- ----------------- -------------
---------
C1                          cluster-network  10.10.1.103
NX3232C

     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I6(1)
    Version Source: CDP

C2                          cluster-network  10.10.1.104
NX3232C

      Serial Number: FOX000002
       Is Monitored: true
             Reason:
```

```
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I6(1)
    Version Source: CDP
CL1                         cluster-network  10.10.1.101   CN1610

     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP
CL2                         cluster-network  10.10.1.102
CN1610

     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP 4 entries were displayed.
```

3. Extrair os CN1610 interrutores substituídos, se não forem removidos automaticamente:

   `system cluster-switch delete -device switch-name`

   Mostrar exemplo

   Você deve excluir ambos os dispositivos individualmente, como mostrado no exemplo a seguir:

   ```
   cluster::> system cluster-switch delete -device CL1
   cluster::> system cluster-switch delete -device CL2
   ```

4. Verifique se os switches de cluster adequados são monitorados:

   `system cluster-switch show`

Mostrar exemplo

O exemplo a seguir mostra que os switches de cluster C1 e C2 estão sendo monitorados:

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C

     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I6(1)
    Version Source: CDP

C2                          cluster-network    10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
          Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I6(1)
    Version Source: CDP

2 entries were displayed.
```

5. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migração de switch Nexus 5596

Migre o fluxo de trabalho dos switches Nexus 5596 para os switches Nexus 3232C

Siga estas etapas do fluxo de trabalho para migrar seus switches Cisco Nexus 5596 para switches Cisco Nexus 3232C.

1 **"Requisitos de migração"**

Revise as informações de exemplo do switch para o processo de migração.

2 **"Prepare-se para a migração"**

Prepare seus switches Nexus 5596 para migração para os switches Nexus 3232C.

3 **"Configure as portas"**

Configure suas portas para migração para os novos switches Nexus 3232C.

4 **"Conclua a migração"**

Conclua a migração para os novos switches Nexus 3232C.

Requisitos de migração

Os switches Cisco Nexus 3232C podem ser usados como switches de cluster no seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Para obter mais informações, consulte:

- "Switches Ethernet Cisco"
- "Hardware Universe"

Cisco Nexus 5596 requisitos

Os switches de cluster usam as seguintes portas para conexões com nós:

- Nexus 5596: Portas E1/1-40 (10 GbE)
- Nexus 3232C: Portas E1/1-30 (10/40/100 GbE)

Os switches do cluster usam as seguintes portas ISL (Inter-Switch Link):

- Nexus 5596: Portas E1/41-48 (10 GbE)
- Nexus 3232C: Portas E1/31-32 (40/100 GbE)

O "*Hardware Universe*" contém informações sobre cabeamento compatível com switches Nexus 3232C:

- Os nós com conexões de cluster de 10 GbE exigem cabos de conexões de fibra ótica QSFP para SFP ou cabos de conexões de cobre QSFP para SFP.
- Os nós com conexões de cluster de 40/100 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.

Os switches de cluster usam o cabeamento ISL apropriado:

- Início: Nexus 5596 (SFP para SFP)
  - 8x cabos de conexão direta de fibra ou cobre SFP
- Interino: Nexus 5596 para Nexus 3232C (QSFP para mais de 4xSFP break-out)
  - 1x cabos de rutura de fibra QSFP para SFP ou de rutura de cobre
- Final: Nexus 3232C ao Nexus 3232C (QSFP28 a QSFP28)
  - 2x QSFP28 cabos de ligação direta de fibra ou cobre
- Nos switches Nexus 3232C, você pode operar portas QSFP/QSFP28 nos modos 40/100 Gigabit Ethernet ou 4 x10 Gigabit Ethernet.

  Por padrão, existem 32 portas no modo 40/100 Gigabit Ethernet. Essas 40 portas Gigabit Ethernet são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta 40 Gigabit Ethernet é numerada como 1/2.

  O processo de alteração da configuração de 40 Gigabit Ethernet para 10 Gigabit Ethernet é chamado *breakout* e o processo de alteração da configuração de 10 Gigabit Ethernet para 40 Gigabit Ethernet é chamado *breakin*.

  Quando você divide uma porta Ethernet de 40/100 Gigabit em 10 portas Gigabit Ethernet, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta 40/100 Gigabit Ethernet são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.
- No lado esquerdo dos switches Nexus 3232C estão 2 portas SFP mais, chamadas 1/33 e 1/34.
- Você configurou algumas das portas nos switches Nexus 3232C para serem executadas a 10 GbE ou 40/100 GbE.

  > Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP a partir da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.
- Você fez o Planejamento, a migração e leu a documentação necessária sobre a conectividade de 10 GbE e 40/100 GbE dos nós para os switches de cluster Nexus 3232C.
- As versões ONTAP e NX-OS suportadas neste procedimento estão em"Switches Ethernet Cisco" .

Sobre os exemplos usados

Os exemplos neste procedimento descrevem a substituição de switches Cisco Nexus 5596 por switches Cisco Nexus 3232C. Você pode usar estas etapas (com modificações) para outras centrais Cisco mais antigas (por exemplo, 3132Q-V).

O procedimento também usa a seguinte nomenclatura de switch e nó:

- As saídas de comando podem variar dependendo de diferentes versões do ONTAP.
- Os switches Nexus 5596 a serem substituídos são **CL1** e **CL2**.
- Os switches Nexus 3232C para substituir os switches Nexus 5596 são **C1** e **C2**.
- **n1_clus1** é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.

- **n1_clus2** é o primeiro cluster LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus3** é o segundo LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus4** é o segundo LIF conetado ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- O número de portas 10 GbE e 40/100 GbE são definidas nos arquivos de configuração de referência (RCFs) disponíveis no"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .
- Os nós são **n1**, **n2**, **n3** e **n4**.

Os exemplos neste procedimento usam quatro nós:

- Dois nós usam quatro portas de interconexão de cluster de 10 GbE: **e0a**, **e0b**, **e0c** e **e0d**.
- Os outros dois nós usam duas portas de interconexão de cluster de 40 GbE: **e4a** e **e4e**.

  A "*Hardware Universe*" lista as portas de cluster reais em suas plataformas.

Cenários abordados

Este procedimento abrange os seguintes cenários:

- O cluster começa com dois nós conectados e funcionando em dois switches de cluster Nexus 5596.
- O interrutor do cluster CL2 a ser substituído por C2 (passos 1 a 19):
  - O tráfego em todas as portas de cluster e LIFs em todos os nós conectados ao CL2 é migrado para as primeiras portas de cluster e LIFs conetadas ao CL1.
  - Desconete o cabeamento de todas as portas de cluster em todos os nós conectados ao CL2 e use o cabeamento de saída compatível para reconetar as portas ao novo switch de cluster C2.
  - Desconete o cabeamento entre as portas ISL entre CL1 e CL2 e, em seguida, use o cabeamento de saída suportado para reconetar as portas de CL1 a C2.
  - O tráfego em todas as portas de cluster e LIFs conetadas ao C2 em todos os nós é revertido.
- O interrutor do cluster CL2 a ser substituído por C2.
  - O tráfego em todas as portas de cluster ou LIFs em todos os nós conectados ao CL1 é migrado para as segundas portas de cluster ou LIFs conetadas ao C2.
  - Desconete o cabeamento de todas as portas de cluster em todos os nós conectados ao CL1 e reconete, usando o cabeamento de saída compatível, ao novo switch de cluster C1.
  - Desconete o cabeamento entre as portas ISL entre CL1 e C2 e reconete usando o cabeamento suportado, de C1 a C2.
  - O tráfego em todas as portas de cluster ou LIFs conetadas ao C1 em todos os nós é revertido.
- Dois nós de FAS9000 foram adicionados ao cluster com exemplos mostrando detalhes do cluster.

O que se segue?

"Prepare-se para a migração".

Prepare-se para a migração de switches Nexus 5596 para switches Nexus 3232C

Siga estas etapas para preparar seus switches Cisco Nexus 5596 para migração para os switches Cisco Nexus 3232C.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   ```
   network device-discovery show
   ```

   Mostrar exemplo

   O exemplo a seguir mostra quantas interfaces de interconexão de cluster foram configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   cluster::> network device-discovery show
              Local  Discovered
   Node       Port   Device               Interface         Platform
   ---------- ------ ------------------ ----------------
   ----------------
   n1         /cdp
              e0a    CL1                  Ethernet1/1       N5K-C5596UP
              e0b    CL2                  Ethernet1/1       N5K-C5596UP
              e0c    CL2                  Ethernet1/2       N5K-C5596UP
              e0d    CL1                  Ethernet1/2       N5K-C5596UP
   n2         /cdp
              e0a    CL1                  Ethernet1/3       N5K-C5596UP
              e0b    CL2                  Ethernet1/3       N5K-C5596UP
              e0c    CL2                  Ethernet1/4       N5K-C5596UP
              e0d    CL1                  Ethernet1/4       N5K-C5596UP
   8 entries were displayed.
   ```

3. Determine o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede:

      ```
      network port show -role cluster
      ```

Mostrar exemplo

O exemplo a seguir exibe os atributos da porta de rede nos nós n1 e n2:

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas:

```
network interface show -role cluster
```

Mostrar exemplo

O exemplo a seguir exibe as informações gerais sobre todas as LIFs no cluster, incluindo suas portas atuais:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------ ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

c. Exibir informações sobre os switches de cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo a seguir mostra os switches do cluster ativo:

```
cluster::*> system cluster-switch show

Switch                        Type               Address
Model
----------------------------- ------------------ ---------------
---------------
CL1                           cluster-network    10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP

2 entries were displayed.
```

4. Verifique se o RCF e a imagem apropriados estão instalados nos novos switches 3232C conforme necessário para seus requisitos e faça as personalizações essenciais do site, como usuários e senhas, endereços de rede e outras personalizações.

   Neste momento, tem de preparar ambos os interrutores.

   Se você precisar atualizar o RCF e a imagem, você deve concluir as seguintes etapas:

   a. Vá para a página *switches Ethernet Cisco* no site de suporte da NetApp.

      "Switches Ethernet Cisco"

   b. Observe o switch e as versões de software necessárias na tabela nessa página.

   c. Baixe a versão apropriada do RCF.

   d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na

página **Download** para baixar o RCF.

e. Transfira a versão apropriada do software de imagem.

Consulte a página *ONTAP 8.x ou mais recente de transferência de Configuração de comutador de rede de Gestão e Cluster_* e, em seguida, selecione a versão apropriada.

Para encontrar a versão correta, consulte a página de download do comutador de rede de cluster *ONTAP 8.x ou posterior*.

5. Migrar os LIFs associados ao segundo switch Nexus 5596 a ser substituído:

`network interface migrate -vserver` *`vserver-name`* `-lif` *`lif-name`* `-source-node` *`source-node-name`* `- destination-node` *`node-name`* `-destination-port` *`destination-port-name`*

Mostrar exemplo

O exemplo a seguir mostra as LIFs sendo migradas para os nós n1 e n2; a migração de LIF deve ser feita em todos os nós:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

6. Verifique a integridade do cluster:

`network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra o status atual de cada cluster:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0a     false
            n1_clus3   up/up      10.10.0.3/24       n1
e0d     false
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0a     false
            n2_clus3   up/up      10.10.0.7/24       n2
e0d     false
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

O que se segue?

"Configure as portas".

Configure suas portas para migração de switches Nexus 5596 para switches Nexus 3232C

Siga estas etapas para configurar suas portas para migração dos switches Nexus 5596 para os novos switches Nexus 3232C.

Passos

1. Encerre as portas de interconexão de cluster que estão fisicamente conetadas ao switch CL2:

   `network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin false`

Mostrar exemplo

Os comandos a seguir desligam as portas especificadas no n1 e no n2, mas as portas devem ser fechadas em todos os nós:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. encerre ISLs 41 a 48 no CL1, o switch Nexus 5596 ativo, usando o comando Cisco `shutdown`.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra ISLs 41 a 48 sendo encerradas no Nexus 5596 switch CL1:

```
(CL1)# configure
(CL1)(Config)# interface e1/41-48
(CL1)(config-if-range)# shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

2. Crie um ISL temporário entre CL1 e C2 usando os comandos Cisco apropriados.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra uma ISL temporária sendo configurada entre CL1 e C2:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

3. Em todos os nós, remova todos os cabos conetados ao switch Nexus 5596 CL2.

   Com o cabeamento compatível, reconecte as portas desconetadas em todos os nós ao switch Nexus 3232C C2.

4. Remova todos os cabos do switch Nexus 5596 CL2.

   Conete o Cisco QSFP apropriado aos cabos de conexão Ethernet 1/24 no novo switch Cisco 3232C, C2, às portas 45 a 48 no Nexus 5596, CL1 existente.

5. Abra as portas ISLs 45 a 48 no switch Nexus 5596 ativo CL1.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de

comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra que as portas ISLs 45 a 48 estão sendo criadas:

```
(CL1)# configure
(CL1)(Config)# interface e1/45-48
(CL1)(config-if-range)# no shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

6. Verifique se os ISLs estão `up` no switch Nexus 5596 CL1.

Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra as portas eth1/45 a eth1/48 indicando (P), o que significa que as portas ISL `up` estão no canal de porta.

```
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/41(D)   Eth1/42(D)
Eth1/43(D)
                                   Eth1/44(D)   Eth1/45(P)
Eth1/46(P)
                                   Eth1/47(P)   Eth1/48(P)
```

7. Verifique se as interfaces eth1/45-48 já têm o modo "Channel-group 1 ativo" em sua configuração em execução.

8. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao switch 3232C C2:

   `network port modify -node node-name -port port-name -up-admin true`

   Mostrar exemplo

   O exemplo a seguir mostra as portas especificadas sendo criadas nos nós n1 e n2:

   ```
   cluster::*> network port modify -node n1 -port e0b -up-admin true
   cluster::*> network port modify -node n1 -port e0c -up-admin true
   cluster::*> network port modify -node n2 -port e0b -up-admin true
   cluster::*> network port modify -node n2 -port e0c -up-admin true
   ```

9. Em todos os nós, reverta todas as LIFs de interconexão de cluster migradas conetadas ao C2:

   `network interface revert -vserver Cluster -lif lif-name`

   Mostrar exemplo

   O exemplo a seguir mostra as LIFs de cluster migradas sendo revertidas para suas portas iniciais:

   ```
   cluster::*> network interface revert -vserver Cluster -lif n1_clus2
   cluster::*> network interface revert -vserver Cluster -lif n1_clus3
   cluster::*> network interface revert -vserver Cluster -lif n2_clus2
   cluster::*> network interface revert -vserver Cluster -lif n2_clus3
   ```

10. Verifique se todas as portas de interconexão de cluster estão agora revertidas para sua casa:

    `network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra que os LIFs no clus2 reverteram para suas portas residenciais e mostra que os LIFs são revertidos com êxito se as portas na coluna porta atual tiverem um status de `true` na `Is Home` coluna. Se o `Is Home` valor for `false`, o LIF não foi revertido.

```
cluster::*> *network interface show -role cluster*
(network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

11. Verifique se as portas em cluster estão conetadas:

    `network port show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra o resultado do comando anterior `network port modify`, verificando se todas as interconexões de cluster são `up`:

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

12. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. em cada nó no cluster, migre as interfaces associadas ao primeiro switch Nexus 5596, CL1, para ser substituído:

   `network interface migrate -vserver` *`vserver-name`* `-lif` *`lif-name`* `-source-node`

source-node-name
-destination-node *destination-node-name* -destination-port *destination-port-name*

Mostrar exemplo

O exemplo a seguir mostra as portas ou LIFs que estão sendo migradas nos nós n1 e n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

2. Verifique o status do cluster:

   ```
   network interface show
   ```

Mostrar exemplo

O exemplo a seguir mostra que as LIFs de cluster necessárias foram migradas para portas de cluster apropriadas hospedadas no switch de cluster, C2:

```
cluster::*> network interface show

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0b     false
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0c     false
            n2_clus1   up/up      10.10.0.5/24       n2
e0b     false
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0c     false
8 entries were displayed.

----- ------- ----
```

3. Em todos os nós, encerre as portas dos nós que estão conectadas ao CL1:

   `network port modify -node *node-name* -port *port-name* -up-admin false`

Mostrar exemplo

O exemplo a seguir mostra as portas especificadas que estão sendo encerradas nos nós n1 e n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

4. Desligue o ISL 24, 31 e 32 no interrutor 3232C ativo C2.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra ISLs sendo encerradas:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if)# exit
C2#
```

5. Em todos os nós, remova todos os cabos conetados ao switch Nexus 5596 CL1.

   Com o cabeamento compatível, reconecte as portas desconetadas em todos os nós ao switch Nexus 3232C C1.

6. Remova o cabo multicondutor QSFP das portas E1/24 do Nexus 3232C C2.

   Conete as portas E1/31 e E1/32 no C1 às portas E1/31 e E1/32 no C2 usando fibra ótica Cisco QSFP ou cabos de conexão direta.

7. Restaure a configuração na porta 24 e remova o Canal de porta temporário 2 no C2.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra a configuração na porta M24 sendo restaurada usando os comandos Cisco apropriados:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

8. Abra as portas ISL 31 e 32 no C2, o switch 3232C ativo, inserindo o seguinte comando Cisco: `no shutdown`

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra os comandos Cisco `switchname configure` apresentados no interrutor 3232C C2:

   ```
   C2# configure
   C2(config)# interface ethernet 1/31-32
   C2(config-if-range)# no shutdown
   ```

9. Verifique se as conexões ISL estão `up` no interrutor 3232C C2.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Referências de comando Cisco Nexus 3000 Series NX-os".

   As portas eth1/31 e eth1/32 devem indicar (P), o que significa que ambas as portas ISL estão no canal de porta

Mostrar exemplo

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

10. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao novo switch 3232C C1:

    `network port modify`

    Mostrar exemplo

    O exemplo a seguir mostra todas as portas de interconexão de cluster sendo criadas para n1 e n2 no switch 3232C C1:

    ```
    cluster::*> network port modify -node n1 -port e0a -up-admin true
    cluster::*> network port modify -node n1 -port e0d -up-admin true
    cluster::*> network port modify -node n2 -port e0a -up-admin true
    cluster::*> network port modify -node n2 -port e0d -up-admin true
    ```

11. Verifique o status da porta do nó do cluster:

    `network port show`

Mostrar exemplo

O exemplo a seguir mostra verifica se todas as portas de interconexão de cluster em todos os nós no novo switch 3232C C1 estão em funcionamento:

```
cluster::*> network port show –role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

12. Em todos os nós, reverta as LIFs de cluster específicas para suas portas iniciais:

```
network interface revert -server Cluster -lif lif-name
```

Mostrar exemplo

O exemplo a seguir mostra as LIFs de cluster específicas sendo revertidas para suas portas iniciais nos nós n1 e n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

13. Verifique se a interface está em casa:

```
network interface show -role cluster
```

Mostrar exemplo

O exemplo a seguir mostra o status das interfaces de interconexão de cluster são `up` e `Is Home` para n1 e n2:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

14. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. expanda o cluster adicionando nós aos switches de cluster Nexus 3232C.

   Os exemplos a seguir mostram que os nós n3 e n4 têm portas de cluster de 40 GbE conetadas às portas E1/7 e E1/8, respetivamente, nos dois switches de cluster Nexus 3232C, e ambos os nós aderiram ao

cluster. As portas de interconexão de cluster de 40 GbE usadas são e4a e e4e.

Exiba as informações sobre os dispositivos em sua configuração:

- `network device-discovery show`
- `network port show -role cluster`
- `network interface show -role cluster`
- `system cluster-switch show`

Mostrar exemplo

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3232C
            e0b    C2                 Ethernet1/1/1    N3K-C3232C
            e0c    C2                 Ethernet1/1/2    N3K-C3232C
            e0d    C1                 Ethernet1/1/2    N3K-C3232C
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3232C
            e0b    C2                 Ethernet1/1/3    N3K-C3232C
            e0c    C2                 Ethernet1/1/4    N3K-C3232C
            e0d    C1                 Ethernet1/1/4    N3K-C3232C
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3232C
            e4e    C2                 Ethernet1/7      N3K-C3232C
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3232C
            e4e    C2                 Ethernet1/8      N3K-C3232C
12 entries were displayed.
```

E

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
```

```
-

Node: n2

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
```

```
-
12 entries were displayed.
```

E

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

E

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                           cluster-network   10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP

4 entries were displayed.
```

2. Extrair o Nexus 5596 substituído com `system cluster-switch delete` o comando, se não for extraído automaticamente:

   `system cluster-switch delete -device switch-name`

   Mostrar exemplo

   ```
   cluster::> system cluster-switch delete -device CL1
   cluster::> system cluster-switch delete -device CL2
   ```

O que se segue?

"Conclua a migração".

Conclua sua migração de 5596 switches para 3232C switches

Conclua as etapas a seguir para finalizar a migração de switches Nexus 5596 para os switches Nexus 3232C.

Passos

1. Verifique se os switches de cluster adequados são monitorados:

   `system cluster-switch show`

Mostrar exemplo

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network    10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

2. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migrar de clusters sem switch de dois nós

Migrar de um fluxo de trabalho de cluster sem switch de dois nós

Siga estas etapas do fluxo de trabalho para migrar de um cluster sem switch de dois nós para um cluster com switches de cluster Cisco Nexus 3232C.

1 **"Requisitos de migração"**

Revise as informações de exemplo do switch para o processo de migração.

2 **"Prepare-se para a migração"**

Prepare seu cluster sem switch de dois nós para migração para um cluster comutado de dois nós.

3 **"Configure as portas"**

Configure o cluster sem switch de dois nós para migração para um cluster comutado de dois nós.

4 **"Conclua a migração"**

Conclua a migração para um cluster comutado de dois nós.

Requisitos de migração

Se você tiver um cluster sem switch de dois nós, poderá migrar para um cluster comutado de dois nós que inclui os switches de rede de cluster Cisco Nexus 3232C. Este é um procedimento sem interrupções.

Antes de começar

Verifique as seguintes instalações e conexões:

- As portas estão disponíveis para conexões de nós. Os switches do cluster usam as portas ISL (Inter-Switch Link) E1/31-32.
- Você tem cabos apropriados para conexões de cluster:
  - Os nós com conexões de cluster de 10 GbE exigem módulos óticos QSFP com cabos de fibra de fuga ou cabos de ligação de cobre QSFP para SFP.
  - Os nós com conexões de cluster de 40/100 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.
  - Os switches do cluster exigem o cabeamento ISL apropriado:
    - 2x QSFP28 cabos de ligação direta de fibra ou cobre.
- As configurações estão corretamente configuradas e funcionando.

  Os dois nós devem estar conetados e funcionando em uma configuração de cluster sem switch de dois nós.

- Todas as portas de cluster estão no estado **up**.
- O switch de cluster Cisco Nexus 3232C é compatível.
- A configuração de rede de cluster existente tem o seguinte:
  - Uma infraestrutura de cluster Nexus 3232C redundante e totalmente funcional em ambos os switches
  - As versões mais recentes do RCF e NX-os em seus switches
  - Conetividade de gerenciamento em ambos os switches

- Acesso ao console a ambos os switches
- Todas as interfaces lógicas de cluster (LIFs) no estado **up** sem terem sido migradas
- Personalização inicial do switch
- Todas as portas ISL ativadas e cabeadas

Sobre os exemplos usados

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Switches de cluster Nexus 3232C, **C1** e **C2**.
- Os nós são **n1** e **n2**.

Os exemplos neste procedimento usam dois nós, cada um usando duas portas de interconexão de cluster de 40 GbE **e4a** e **e4e**. "*Hardware Universe*"O tem detalhes sobre as portas de cluster em suas plataformas.

- **n1_clus1** é a primeira interface lógica de cluster (LIF) a ser conetada ao switch de cluster **C1** para o nó **n1**.
- **n1_clus2** é o primeiro cluster LIF a ser conetado ao switch de cluster **C2** para o nó **n1**.
- **n2_clus1** é o primeiro cluster LIF a ser conetado ao switch de cluster **C1** para o nó **n2**.
- **n2_clus2** é o segundo cluster LIF a ser conetado ao switch de cluster **C2** para o nó **n2**.
- O número de portas 10 GbE e 40/100 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis na "Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" página.

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

O que se segue?

"Prepare-se para a migração".

Prepare-se para a migração de clusters sem switch de dois nós para clusters comutados de dois nós

Siga estas etapas para preparar seu cluster sem switch de dois nós para migrar para um cluster comutado de dois nós que inclui os switches de rede de cluster Cisco Nexus 3232C.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Determine o status administrativo ou operacional de cada interface de cluster:

a. Exibir os atributos da porta de rede:

```
network port show -role cluster
```

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
4 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas e seus nós iniciais designados:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------ ------- ---
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true

4 entries were displayed.
```

c. Verifique se a deteção de cluster sem switch está ativada usando o comando de privilégio avançado:

`network options detect-switchless-cluster show`

Mostrar exemplo

A saída no exemplo a seguir mostra que a deteção de cluster sem switch está ativada:

```
cluster::*> network options detect-switchless-cluster show
Enable Switchless Cluster Detection: true
```

3. Verifique se os RCFs e a imagem apropriados estão instalados nos novos switches 3232C e faça as personalizações necessárias do site, como adicionar usuários, senhas e endereços de rede.

   Neste momento, tem de preparar ambos os interrutores. Se você precisar atualizar o RCF e o software de imagem, siga estas etapas:

   a. Vá para a página *switches Ethernet Cisco* no site de suporte da NetApp.

      "Switches Ethernet Cisco"

   b. Observe o switch e as versões de software necessárias na tabela nessa página.

   c. Baixe a versão apropriada do RCF.

d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.

e. Transfira a versão apropriada do software de imagem.

"Download do arquivo de configuração de referência do Cisco Cluster and Management Network Switch"

4. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
5. Nos switches Nexus 3232C C1 e C2, desative todas as portas C1 e C2 voltadas para o nó, mas não desative as portas ISL E1/31-32.

   Para obter mais informações sobre comandos Cisco, consulte a lista a seguir no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   O exemplo a seguir mostra que as portas 1 a 30 estão sendo desativadas nos switches de cluster Nexus 3232C C1 e C2 usando uma configuração suportada no RCF : `NX3232_RCF_v1.0_24p10g_24p100g.txt`

   ```
   C1# copy running-config startup-config
   [] 100% Copy complete.
   C1# configure
   C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
   4,e1/7-30
   C1(config-if-range)# shutdown
   C1(config-if-range)# exit
   C1(config)# exit
   C2# copy running-config startup-config
   [] 100% Copy complete.
   C2# configure
   C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
   4,e1/7-30
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# exit
   ```

6. Conete as portas 1/31 e 1/32 no C1 às mesmas portas no C2 usando cabeamento compatível.
7. Verifique se as portas ISL estão operacionais no C1 e C2:

   ```
   show port-channel summary
   ```

   Para obter mais informações sobre comandos Cisco, consulte a lista a seguir no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra o comando Cisco `show port-channel summary` que está sendo usado para verificar se as portas ISL estão operacionais no C1 e no C2:

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)        s -
Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
      Port-
Group Channel      Type   Protocol  Member Ports
------------------------------------------------------------------------
-----------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)

C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)        s -
Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------

Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

8. Exiba a lista de dispositivos vizinhos no switch.

   Para obter mais informações sobre comandos Cisco, consulte a lista a seguir no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra o comando Cisco `show cdp neighbors` que está sendo usado para exibir os dispositivos vizinhos no switch:

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                 Eth1/31        174    R S I s     N3K-C3232C
Eth1/31
C2                 Eth1/32        174    R S I s     N3K-C3232C
Eth1/32
Total entries displayed: 2
C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                 Eth1/31        178    R S I s     N3K-C3232C
Eth1/31
C1                 Eth1/32        178    R S I s     N3K-C3232C
Eth1/32
Total entries displayed: 2
```

9. Exiba a conetividade da porta do cluster em cada nó:

   `network device-discovery show`

Mostrar exemplo

O exemplo a seguir mostra a conetividade da porta do cluster exibida para uma configuração de cluster sem switch de dois nós:

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ -------------------- ---------------- ----------------
n1         /cdp
            e4a    n2                   e4a              FAS9000
            e4e    n2                   e4e              FAS9000
n2         /cdp
            e4a    n1                   e4a              FAS9000
            e4e    n1                   e4e              FAS9000
```

O que se segue?

"Configure as portas".

Configure suas portas para migração de um cluster sem switch de dois nós para um cluster comutado de dois nós

Siga estas etapas para configurar suas portas para migração de um cluster sem switch de dois nós para um cluster comutado de dois nós em switches Nexus 3232C.

Passos

1. Migre as LIFs n1_clus1 e n2_clus1 para as portas físicas de seus nós de destino:

   `network interface migrate -vserver` *`vserver-name`* `-lif` *`lif-name`* `source-node` *`source-node-name`* `-destination-port` *`destination-port-name`*

   Mostrar exemplo

   Você deve executar o comando para cada nó local como mostrado no exemplo a seguir:

   ```
   cluster::*> network interface migrate -vserver cluster -lif n1_clus1
   -source-node n1
   -destination-node n1 -destination-port e4e
   cluster::*> network interface migrate -vserver cluster -lif n2_clus1
   -source-node n2
   -destination-node n2 -destination-port e4e
   ```

2. Verifique se as interfaces do cluster migraram com êxito:

   `network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra o status "está Home" para os LIFs n1_clus1 e n2_clus1 se tornou "false" após a migração ser concluída:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4e     false
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4e     false
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
 4 entries were displayed.
```

3. Encerre as portas do cluster para as LIFs n1_clus1 e n2_clus1, que foram migradas na etapa 9:

   `network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin false`

   Mostrar exemplo

   Você deve executar o comando para cada porta como mostrado no exemplo a seguir:

   ```
   cluster::*> network port modify -node n1 -port e4a -up-admin false
   cluster::*> network port modify -node n2 -port e4a -up-admin false
   ```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1        e4a    10.10.0.1
Cluster n1_clus2 n1        e4e    10.10.0.2
Cluster n2_clus1 n2        e4a    10.10.0.3
Cluster n2_clus2 n2        e4e    10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s) ................
Detected 9000 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. Desconete o cabo do e4a no nó n1.

   Você pode consultar a configuração em execução e conetar a primeira porta de 40 GbE no switch C1 (porta 1/7 neste exemplo) a e4a no n1 usando cabeamento compatível com switches Nexus 3232C.

2. Desconete o cabo do e4a no nó n2.

   Você pode consultar a configuração em execução e conetar o e4a à próxima porta de 40 GbE disponível no C1, porta 1/8, usando o cabeamento suportado.

3. Habilite todas as portas voltadas para nós no C1.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 30 estão sendo habilitadas nos switches de cluster Nexus 3232C C1 e C2 usando a configuração suportada no RCF : `NX3232_RCF_v1.0_24p10g_26p100g.txt`

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

4. Ative a primeira porta de cluster, e4a, em cada nó:

   `network port modify -node node-name -port port-name -up-admin true`

   Mostrar exemplo

   ```
   cluster::*> network port modify -node n1 -port e4a -up-admin true
   cluster::*> network port modify -node n2 -port e4a -up-admin true
   ```

5. Verifique se os clusters estão ativos em ambos os nós:

   `network port show -role cluster`

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -

4 entries were displayed.
```

6. Para cada nó, reverta todas as LIFs de interconexão de cluster migradas:

   `network interface revert -vserver cluster -lif` *`lif-name`*

Mostrar exemplo

Você deve reverter cada LIF para sua porta inicial individualmente, como mostrado no exemplo a seguir:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus1
```

7. Verifique se todos os LIFs agora são revertidos para suas portas residenciais:

   `network interface show -role cluster`

   A `Is Home` coluna deve exibir um valor de `true` para todas as portas listadas na `Current Port` coluna. Se o valor exibido for `false`, a porta não foi revertida.

   Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

8. Exiba a conetividade da porta do cluster em cada nó:

   `network device-discovery show`

Mostrar exemplo

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3232C
            e4e    n2                 e4e              FAS9000
n2         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3232C
            e4e    n1                 e4e              FAS9000
```

9. Migre clus2 para a porta e4a no console de cada nó:

   `network interface migrate cluster -lif` *`lif-name`* `-source-node` *`source-node-name`* `-destination-node` *`destination-node-name`* `-destination-port` *`destination-port-name`*

   Mostrar exemplo

   Você deve migrar cada LIF para sua porta inicial individualmente, como mostrado no exemplo a seguir:

   ```
   cluster::*> network interface migrate -vserver cluster -lif n1_clus2
   -source-node n1
   -destination-node n1 -destination-port e4a
   cluster::*> network interface migrate -vserver cluster -lif n2_clus2
   -source-node n2
   -destination-node n2 -destination-port e4a
   ```

10. Encerre as portas de cluster clus2 LIF em ambos os nós:

    `network port modify`

    Mostrar exemplo

    O exemplo a seguir mostra as portas especificadas que estão sendo definidas como `false`, fechando as portas em ambos os nós:

    ```
    cluster::*> network port modify -node n1 -port e4e -up-admin false
    cluster::*> network port modify -node n2 -port e4e -up-admin false
    ```

11. Verifique o status de LIF do cluster:

    `network interface show`

    Mostrar exemplo

    ```
    cluster::*> network interface show -role cluster
     (network interface show)
                Logical    Status     Network            Current
    Current Is
    Vserver     Interface  Admin/Oper Address/Mask       Node
    Port    Home
    ----------- ---------- ---------- ------------------ -------------
    ------- ----
    Cluster
                n1_clus1   up/up      10.10.0.1/24       n1
    e4a     true
                n1_clus2   up/up      10.10.0.2/24       n1
    e4a     false
                n2_clus1   up/up      10.10.0.3/24       n2
    e4a     true
                n2_clus2   up/up      10.10.0.4/24       n2
    e4a     false
    4 entries were displayed.
    ```

12. Desconete o cabo do e4e no nó n1.

    Você pode consultar a configuração em execução e conetar a primeira porta de 40 GbE no switch C2 (porta 1/7 neste exemplo) a e4e no nó n1, usando o cabeamento apropriado para o modelo de switch Nexus 3232C.

13. Desconete o cabo do e4e no nó n2.

    Você pode consultar a configuração em execução e conetar o e4e à próxima porta de 40 GbE disponível no C2, porta 1/8, usando o cabeamento apropriado para o modelo de switch Nexus 3232C.

14. Habilite todas as portas voltadas para nós no C2.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 30 estão sendo habilitadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração suportada no RCF : `NX3232C_RCF_v1.0_24p10g_26p100g.txt`

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

15. Ative a segunda porta do cluster, e4e, em cada nó:

`network port modify`

Mostrar exemplo

O exemplo a seguir mostra a segunda porta de cluster e4e sendo criada em cada nó:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> *network port modify -node n2 -port e4e -up-admin true*s
```

16. Para cada nó, reverta todas as LIFs de interconexão de cluster migradas:

`network interface revert`

Mostrar exemplo

O exemplo a seguir mostra os LIFs migrados sendo revertidos para suas portas residenciais.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

O que se segue?

"Conclua a migração".

Conclua a migração de um cluster sem switch de dois nós para um cluster comutado de dois nós

Conclua as etapas a seguir para finalizar a migração de cluster sem switch de dois nós para um cluster comutado de dois nós nos switches Nexus 3232C.

Passos

1. Verifique se todas as portas de interconexão de cluster estão agora revertidas para suas portas iniciais:

   `network interface show -role cluster`

   A `Is Home` coluna deve exibir um valor de `true` para todas as portas listadas na `Current Port` coluna. Se o valor exibido for `false`, a porta não foi revertida.

   Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

2. Verifique se todas as portas de interconexão de cluster estão no `up` estado:

   `network port show -role cluster`

3. Exiba os números da porta do switch de cluster através da qual cada porta do cluster está conetada a cada nó:

   `network device-discovery show`

Mostrar exemplo

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1          /cdp
            e4a    C1                 Ethernet1/7      N3K-C3232C
            e4e    C2                 Ethernet1/7      N3K-C3232C
n2          /cdp
            e4a    C1                 Ethernet1/8      N3K-C3232C
            e4e    C2                 Ethernet1/8      N3K-C3232C
```

4. Exibir switches do cluster descobertos e monitorados:

   `system cluster-switch show`

Mostrar exemplo

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.101
NX3232CV
Serial Number: FOX000001
Is Monitored: true
Reason:
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version 7.0(3)I6(1)
Version Source: CDP

C2                          cluster-network     10.10.1.102
NX3232CV
Serial Number: FOX000002
Is Monitored: true
Reason:
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version 7.0(3)I6(1)
Version Source: CDP 2 entries were displayed.
```

5. Verifique se a deteção de cluster sem switch alterou a opção de cluster sem switch para desativada:

   ```
   network options switchless-cluster show
   ```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1        e4a    10.10.0.1
Cluster n1_clus2 n1        e4e    10.10.0.2
Cluster n2_clus1 n2        e4a    10.10.0.3
Cluster n2_clus2 n2        e4e    10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s) ................
Detected 9000 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os interrutores

Substitua um switch de cluster Cisco Nexus 3232C

Siga estas etapas para substituir um switch Cisco Nexus 3232C com defeito em um cluster. Este é um procedimento sem interrupções.

Rever os requisitos

O que você vai precisar

Certifique-se de que o cluster e a configuração de rede existentes tenham as seguintes caraterísticas:

- A infraestrutura de cluster do Nexus 3232C é redundante e totalmente funcional em ambos os switches.

  A página de switches Ethernet Cisco tem as versões mais recentes de RCF e NX-os em seus switches.

- Todas as portas de cluster devem estar no estado **up**.

- A conetividade de gerenciamento deve existir em ambos os switches.
- Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e não são migradas.

O interrutor de substituição Cisco Nexus 3232C tem as seguintes caraterísticas:

- A conetividade de rede de gerenciamento é funcional.
- O acesso do console ao interrutor de substituição está no lugar.
- A imagem apropriada do sistema operacional RCF e NX-os é carregada no switch.
- A personalização inicial do switch está concluída.

Para mais informações

Veja o seguinte:

- "Switches Ethernet Cisco"
- "Hardware Universe"

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desabilitar a criação de casos durante a manutenção. Veja este artigo da Base de Conhecimento"SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para mais detalhes.
- Habilite o registro de sessão para qualquer sessão CLI. Para obter instruções sobre como habilitar o registro de sessão, revise a seção "Registro de saída de sessão" neste artigo da Base de conhecimento"Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Substitua o interrutor

Sobre esta tarefa

Este procedimento de substituição descreve o seguinte cenário:

- Inicialmente, o cluster tem quatro nós conectados a dois switches de cluster Nexus 3232C, CL1 e CL2.
- Pretende substituir o interrutor do cluster CL2 por C2 (passos 1 a 21):
  - Em cada nó, você migra as LIFs de cluster conetadas ao switch de cluster CL2 para as portas de cluster conetadas ao switch de cluster CL1.
  - Desconete o cabeamento de todas as portas do switch de cluster CL2 e reconete o cabeamento às mesmas portas do switch de cluster de substituição C2.
  - Você reverte as LIFs de cluster migradas em cada nó.

Sobre os exemplos

Este procedimento de substituição substitui o segundo switch de cluster Nexus 3232C CL2 com o novo switch 3232C C2.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os quatro nós são n1, n2, n3 e n4.

- N1_clus1 é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster C1 para o nó n1.
- N1_clus2 é o primeiro cluster LIF conetado ao switch de cluster CL2 ou C2 para o nó n1.
- N1_clus3 é o segundo LIF conetado ao switch de cluster C2 para o nó n1.-
- N1_clus4 é o segundo LIF conetado ao switch de cluster CL1, para o nó n1.

O número de portas de 10 GbE e 40/100 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .

Os exemplos neste procedimento de substituição usam quatro nós. Dois dos nós usam quatro portas de interconexão de cluster de 10 GB: e0a, e0b, e0c e e0d. Os outros dois nós usam duas portas de interconexão de cluster de 40 GB: e4a e e4e. Consulte "Hardware Universe"para verificar as portas de cluster corretas para a sua plataforma.

Etapa 1: Exiba e migre as portas do cluster para o switch

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface         Platform
----------- ------ -------------------- ----------------
----------------
n1         /cdp
            e0a    CL1                  Ethernet1/1/1    N3K-C3232C
            e0b    CL2                  Ethernet1/1/1    N3K-C3232C
            e0c    CL2                  Ethernet1/1/2    N3K-C3232C
            e0d    CL1                  Ethernet1/1/2    N3K-C3232C

n2         /cdp
            e0a    CL1                  Ethernet1/1/3    N3K-C3232C
            e0b    CL2                  Ethernet1/1/3    N3K-C3232C
            e0c    CL2                  Ethernet1/1/4    N3K-C3232C
            e0d    CL1                  Ethernet1/1/4    N3K-C3232C

n3         /cdp
            e4a    CL1                  Ethernet1/7      N3K-C3232C
            e4e    CL2                  Ethernet1/7      N3K-C3232C

n4         /cdp
            e4a    CL1                  Ethernet1/8      N3K-C3232C
            e4e    CL2                  Ethernet1/8      N3K-C3232C
```

3. Determine o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede:

      `network port show -role cluster`

Mostrar exemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
------------
e0a       Cluster      Cluster          up   9000 auto/10000  -
e0b       Cluster      Cluster          up   9000 auto/10000  -
e0c       Cluster      Cluster          up   9000 auto/10000  -
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
------------
e0a       Cluster      Cluster          up   9000  auto/10000 -
e0b       Cluster      Cluster          up   9000  auto/10000 -
e0c       Cluster      Cluster          up   9000  auto/10000 -
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
```

```
-

Node: n4

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
```

b. Exibir informações sobre as interfaces lógicas (LIFs):

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster::*> network interface show -role cluster
             Logical    Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port   Home
----------- ---------- ---------- ------------------
------------ ------- ---
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true
```

c. Exibir os switches do cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo de saída a seguir exibe os switches de cluster:

```
cluster::> system cluster-switch show
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                         cluster-network    10.10.1.101
NX3232C
        Serial Number: FOX000001
         Is Monitored: true
               Reason: None
     Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
       Version Source: CDP

CL2                         cluster-network    10.10.1.102
NX3232C
        Serial Number: FOX000002
         Is Monitored: true
               Reason: None
     Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
       Version Source: CDP
```

4. Verifique se o RCF e a imagem apropriados estão instalados no novo switch Nexus 3232C e faça as personalizações necessárias do local.
   a. Vá para o site de suporte da NetApp.

      "mysupport.NetApp.com"

   b. Vá para a página **switches Ethernet Cisco** e anote as versões de software necessárias na tabela.

      "Switches Ethernet Cisco"

   c. Baixe a versão apropriada do RCF.
   d. Clique em **CONTINUAR** na página **Descrição**, aceite o contrato de licença e navegue até a página **Download**.
   e. Transfira a versão correta do software de imagem a partir da página de transferência do ficheiro de configuração de referência do comutador de rede de gestão e de Cluster **Cisco**.

      "Download do arquivo de configuração de referência do comutador de rede de gerenciamento e cluster Cisco"

5. Migre as LIFs de cluster para as portas de nó físico conetadas ao switch de substituição C2:

`network interface migrate -vserver vserver-name -lif lif-name -source-node node-name -destination-node node-name -destination-port port-name`

Mostrar exemplo

Você deve migrar todas as LIFs de cluster individualmente, conforme mostrado no exemplo a seguir:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -destination-
node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -destination-
node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -destination-
node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -destination-
node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 -destination-
node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 -destination-
node n4 -destination-port e4a
```

6. Verifique o estado das portas do cluster e respetivas designações de origem:

   `network interface show -role cluster`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
(network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0a     false
            n1_clus3   up/up      10.10.0.3/24       n1
e0d     false
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0a     false
            n2_clus3   up/up      10.10.0.7/24       n2
e0d     false
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4a     false
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4a     false
```

7. Encerre as portas de interconexão do cluster que estão fisicamente conetadas ao switch original CL2:

   `network port modify -node` *`node-name`* `-port` *`port-name`* `-up-admin false`

Mostrar exemplo

O exemplo a seguir mostra que as portas de interconexão de cluster estão fechadas em todos os nós:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none
.
.
n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
.
.
n3
.
.
.n4
.
.
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1        e0a    10.10.0.1
Cluster n1_clus2 n1        e0b    10.10.0.2
Cluster n1_clus3 n1        e0c    10.10.0.3
Cluster n1_clus4 n1        e0d    10.10.0.4
Cluster n2_clus1 n2        e0a    10.10.0.5
Cluster n2_clus2 n2        e0b    10.10.0.6
Cluster n2_clus3 n2        e0c    10.10.0.7
Cluster n2_clus4 n2        e0d    10.10.0.8
Cluster n3_clus1 n4        e0a    10.10.0.9
Cluster n3_clus2 n3        e0e    10.10.0.10
Cluster n4_clus1 n4        e0a    10.10.0.11
Cluster n4_clus2 n4        e0e    10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11
10.10.0.12 Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) ................
Detected 9000 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
```

```
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Passo 2: Migrar ISLs para o switch CL1 e C2

1. Encerre as portas 1/31 e 1/32 no interrutor do cluster CL1.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   Mostrar exemplo

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/31-32
   (CL1)(config-if-range)# shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

2. Remova todos os cabos conetados ao switch do cluster CL2 e reconete-os ao switch de substituição C2 para todos os nós.
3. Retire os cabos de ligação entre interrutores (ISL) das portas E1/31 e E1/32 no interrutor do cluster CL2 e volte a ligá-los às mesmas portas no interrutor de substituição C2.
4. Abra as portas ISL 1/31 e 1/32 no interrutor do cluster CL1.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

```
(CL1)# configure
(CL1)(Config)# interface e1/31-32
(CL1)(config-if-range)# no shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

5. Verifique se os ISLs estão acima em CL1.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

   As portas eth1/31 e eth1/32 devem indicar `(P)`, o que significa que as portas ISL estão no canal de porta:

   Mostrar exemplo

```
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

6. Verifique se os ISLs estão ativos no switch de cluster C2.

   Para obter mais informações sobre comandos Cisco, consulte os guias listados no "Referências de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

As portas eth1/31 e eth1/32 devem indicar (P), o que significa que ambas as portas ISL estão no canal de porta.

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)        s -
Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

7. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao switch de substituição C2:

   `network port modify -node node-name -port port-name -up-admin true`

Mostrar exemplo

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

Passo 3: Reverter todos os LIFs para portas originalmente atribuídas

1. Reverter todas as LIFs de interconexão de cluster migradas em todos os nós:

   `network interface revert -vserver cluster -lif lif-name`

Mostrar exemplo

Você deve reverter todas as LIFs de interconexão de cluster individualmente, conforme mostrado no exemplo a seguir:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
Cluster::*> network interface revert -vserver cluster -lif n3_clus2
Cluster::*> network interface revert -vserver cluster -lif n4_clus2
```

2. Verifique se as portas de interconexão de cluster estão agora revertidas para sua casa:

   ```
   network interface show
   ```

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs foram revertidos com sucesso porque as portas listadas na `Current Port` coluna têm um status de `true` na `Is Home` coluna. Se uma porta tiver um valor de `false`, o LIF não foi revertido.

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
             n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
             n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
             n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
             n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
             n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
             n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
             n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
             n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
             n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
             n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
             n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
             n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
```

3. Verifique se as portas do cluster estão conetadas:

   `network port show -role cluster`

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000 auto/10000  -
e0b       Cluster      Cluster          up   9000 auto/10000  -
e0c       Cluster      Cluster          up   9000 auto/10000  -
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
 --------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000 -
e0b       Cluster      Cluster          up   9000  auto/10000 -
e0c       Cluster      Cluster          up   9000  auto/10000 -
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
Node: n3

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
Node: n4
```

```
Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2-clus1
none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2
none
.
.
n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1
none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2
none
.
.
n3
.
.
.n4
.
.
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1        e0a    10.10.0.1
Cluster n1_clus2 n1        e0b    10.10.0.2
Cluster n1_clus3 n1        e0c    10.10.0.3
Cluster n1_clus4 n1        e0d    10.10.0.4
Cluster n2_clus1 n2        e0a    10.10.0.5
Cluster n2_clus2 n2        e0b    10.10.0.6
Cluster n2_clus3 n2        e0c    10.10.0.7
Cluster n2_clus4 n2        e0d    10.10.0.8
Cluster n3_clus1 n4        e0a    10.10.0.9
Cluster n3_clus2 n3        e0e    10.10.0.10
Cluster n4_clus1 n4        e0a    10.10.0.11
Cluster n4_clus2 n4        e0e    10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11
10.10.0.12 Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) ................
Detected 9000 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
```

```
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Etapa 4: Verifique se todas as portas e o LIF estão migrados corretamente

1. Exiba as informações sobre os dispositivos em sua configuração digitando os seguintes comandos:

   Você pode executar os seguintes comandos em qualquer ordem:

   - `network device-discovery show`
   - `network port show -role cluster`
   - `network interface show -role cluster`
   - `system cluster-switch show`

Mostrar exemplo

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3232C
            e0b    C2                 Ethernet1/1/1    N3K-C3232C
            e0c    C2                 Ethernet1/1/2    N3K-C3232C
            e0d    C1                 Ethernet1/1/2    N3K-C3232C
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3232C
            e0b    C2                 Ethernet1/1/3    N3K-C3232C
            e0c    C2                 Ethernet1/1/4    N3K-C3232C
            e0d    C1                 Ethernet1/1/4    N3K-C3232C
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3232C
            e4e    C2                 Ethernet1/7      N3K-C3232C

n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3232C
            e4e    C2                 Ethernet1/8      N3K-C3232C

cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                      Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000 auto/10000  -
e0b       Cluster      Cluster          up   9000 auto/10000  -
e0c       Cluster      Cluster          up   9000 auto/10000  -
e0d       Cluster      Cluster          up   9000 auto/10000  -

Node: n2

Ignore
                                                      Speed(Mbps) Health
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/10000 -
e0b       Cluster      Cluster          up   9000  auto/10000 -
e0c       Cluster      Cluster          up   9000  auto/10000 -
e0d       Cluster      Cluster          up   9000  auto/10000 -

Node: n3

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -

Node: n4

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -

cluster::*> network interface show -role cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            nm1_clus1  up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
```

```
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true

cluster::*> system cluster-switch show
Switch                       Type               Address
Model
---------------------------- ------------------ ----------------
---------------
CL1                           cluster-network   10.10.1.101
NX3232C
             Serial Number: FOX000001
              Is Monitored: true
                    Reason: None
          Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
            Version Source: CDP
CL2                           cluster-network   10.10.1.102
NX3232C
             Serial Number: FOX000002
              Is Monitored: true
                    Reason: None
          Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
            Version Source: CDP

C2                            cluster-network    10.10.1.103
NX3232C
             Serial Number: FOX000003
```

```
              Is Monitored: true
                    Reason: None
          Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
            Version Source: CDP 3 entries were displayed.
```

2. Elimine o interrutor de cluster substituído CL2 se não tiver sido removido automaticamente:

   `system cluster-switch delete -device cluster-switch-name`

3. Verifique se os switches de cluster adequados são monitorados:

   `system cluster-switch show`

   Mostrar exemplo

   O exemplo a seguir mostra que os switches do cluster são monitorados porque o `Is Monitored` estado é `true`.

```
cluster::> system cluster-switch show
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                         cluster-network    10.10.1.101
NX3232C
            Serial Number: FOX000001
             Is Monitored: true
                   Reason: None
         Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
           Version Source: CDP

C2                          cluster-network    10.10.1.103
NX3232C
            Serial Number: FOX000002
             Is Monitored: true
                   Reason: None
         Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version 7.0(3)I6(1)
           Version Source: CDP
```

4. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=END`

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os switches de cluster Cisco Nexus 3232C por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

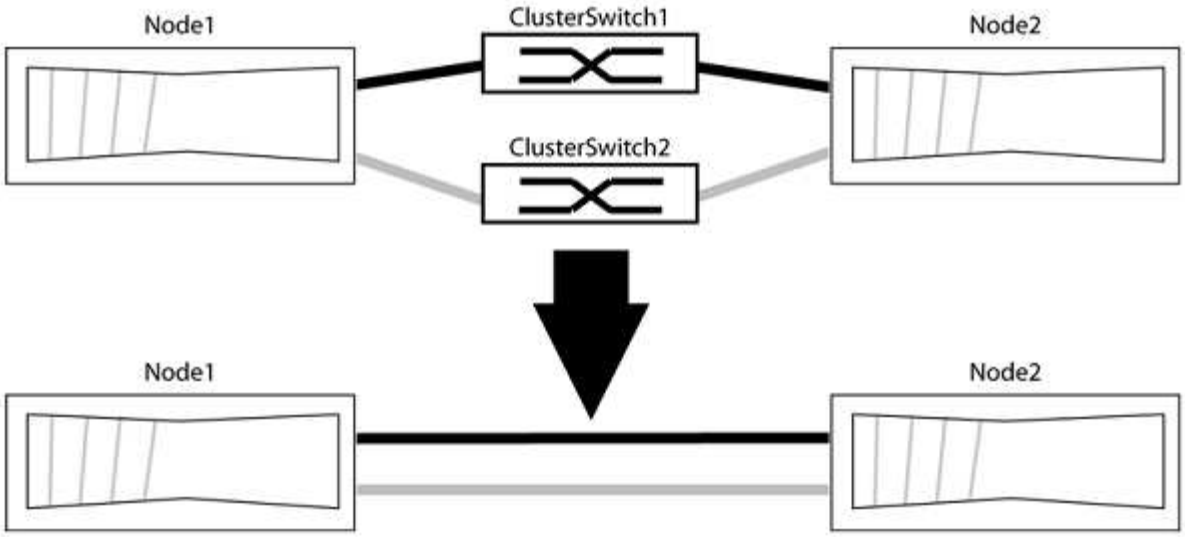
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

   ```
   network options detect-switchless-cluster show
   ```

   Mostrar exemplo

   A saída de exemplo a seguir mostra se a opção está ativada.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

`h`onde está a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico desta tarefa de manutenção para que possa suprimir a criação automática de casos durante a janela de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

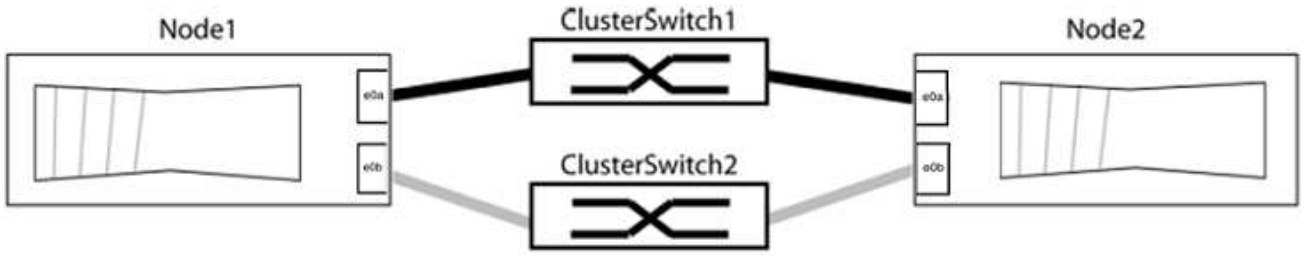
Mostrar exemplo

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-cisco-3232c/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



   Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

   Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

   `network interface show -vserver Cluster -fields is-home`

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

```
network interface revert -vserver Cluster -lif *
```

4. Desativar a reversão automática para as LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

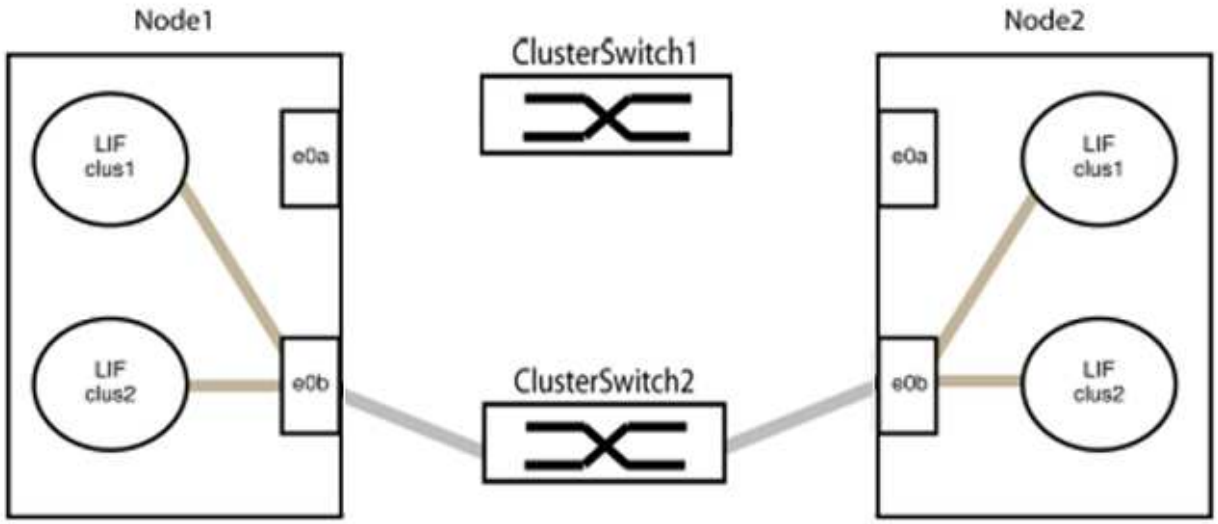
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

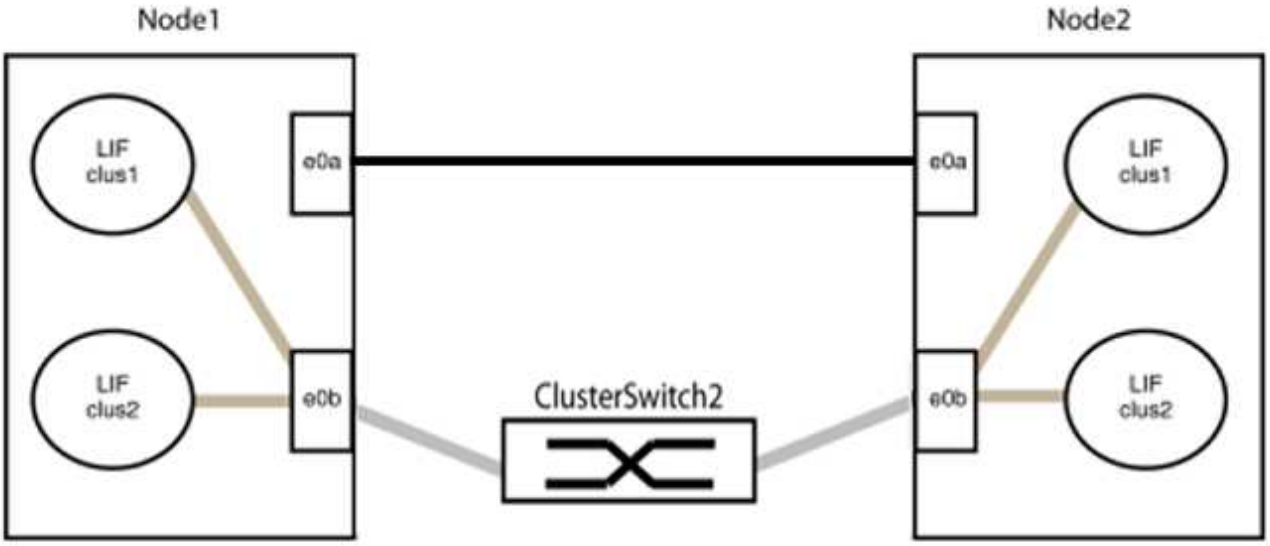
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

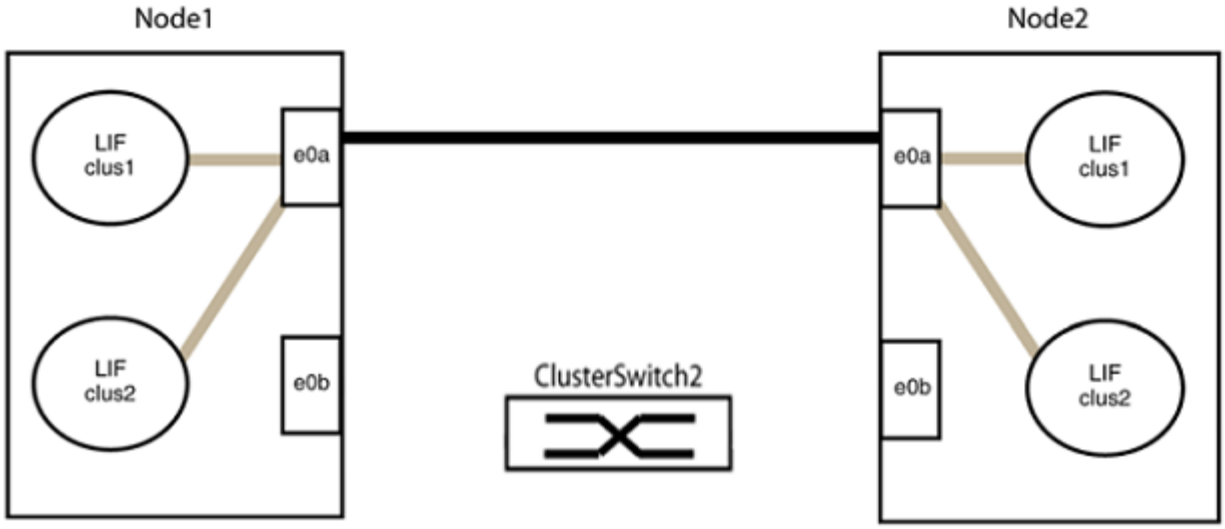
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

Cisco Nexus 3132Q-V

Comece agora

Fluxo de trabalho de instalação e configuração para switches Cisco Nexus 3132Q-V

Os switches Cisco Nexus 3132Q-V podem ser usados como switches de cluster em seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seu switch Cisco Nexus 3132Q-V.

1. **"Requisitos de configuração"**

Revise os requisitos de configuração para o switch de cluster 3132Q-V.

2. **"Documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 3132Q-V e o cluster ONTAP .

3. **"Requisitos para Smart Call Home"**

Revise os requisitos do recurso Cisco Smart Call Home, usado para monitorar os componentes de hardware e software na sua rede.

4. **"Instale o hardware"**

Instale o hardware do switch.

5. **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches Cisco Nexus 3132Q-V.

Para instalação e manutenção do switch Cisco Nexus 3132Q-V, certifique-se de rever os requisitos de rede e configuração.

Requisitos de configuração

Para configurar o cluster, é necessário o número e o tipo apropriados de cabos e conetores de cabos para os switches. Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para o tráfego de rede de gerenciamento.
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis.
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700, a interface e0M utiliza uma porta Ethernet dedicada.

Consulte a "Hardware Universe" para obter informações mais recentes.

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches Cisco Nexus 3132Q-V.

Para instalação e manutenção do switch Cisco Nexus 3132Q-V, certifique-se de rever toda a documentação recomendada.

Documentação do switch

Para configurar os switches Cisco Nexus 3132Q-V, você precisa da seguinte documentação na "Suporte para switches Cisco Nexus 3000 Series" página.

Título do documento	Descrição
Guia de Instalação de hardware da Série Nexus 3000	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
Guias de configuração do software de comutador da série Cisco Nexus 3000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
Guia de atualização e downgrade do software NX-os da série Cisco Nexus 3000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
Cisco Nexus 3000 Series NX-os Guia de Referência de comando	Fornece links para as várias referências de comando fornecidas pelo Cisco.
Cisco Nexus 3000 MIBs Referência	Descreve os arquivos MIB (Management Information base) para os switches Nexus 3000.
Nexus 3000 Series NX-os System Message Reference	Descreve as mensagens do sistema para os switches da série Cisco Nexus 3000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de lançamento do Cisco Nexus 3000 Series NX-os (escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 3000 Series.

Título do documento	Descrição
Informações regulamentares, de conformidade e de segurança para o Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series e Cisco Nexus 2000 Series	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 3000.

Documentação de sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para sua versão do sistema operacional "ONTAP 9" .

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.
Documentação do ONTAP	Fornece informações detalhadas sobre todos os aspetos das versões do ONTAP.
"Hardware Universe"	Fornece informações de compatibilidade e configuração de hardware NetApp.

Kit de trilho e documentação do gabinete

Para instalar um switch Cisco de 3132Q V em um gabinete NetApp, consulte a documentação de hardware a seguir.

Nome	Descrição
"Armário do sistema 42U, guia profundo"	Descreve as FRUs associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição da FRU.
"Instale o switch Cisco Nexus 3132Q-V em um gabinete NetApp"	Descreve como instalar um switch Cisco Nexus 3132Q-V em um gabinete NetApp de quatro colunas.

Requisitos para Smart Call Home

Para usar o Smart Call Home, você deve configurar um switch de rede de cluster para se comunicar por e-mail com o sistema Smart Call Home. Além disso, você pode opcionalmente configurar seu switch de rede de cluster para aproveitar o recurso de suporte Smart Call Home incorporado da Cisco.

O Smart Call Home monitora os componentes de hardware e software na sua rede. Quando ocorre uma configuração crítica do sistema, ele gera uma notificação por e-mail e envia um alerta para todos os destinatários configurados no seu perfil de destino.

Antes de usar o Smart Call Home, esteja ciente dos seguintes requisitos:

- Um servidor de e-mail deve estar no lugar.
- O switch deve ter conetividade IP com o servidor de e-mail.
- É necessário configurar o nome do contacto (contacto do servidor SNMP), o número de telefone e as informações do endereço da rua. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID de CCO deve ser associado a um contrato de serviço Cisco SMARTnet apropriado para a sua empresa.
- O Serviço SMARTnet da Cisco deve estar em vigor para que o dispositivo seja registrado.

O "Site de suporte da Cisco" contém informações sobre os comandos para configurar Smart Call Home.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches Cisco Nexus 3132Q-V

Para instalar e configurar o hardware de um switch de cluster 3132Q-V, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2. **"Instale o interrutor"**

Instale o switch 3132Q-V.

3. **"Instale o interrutor em um gabinete NetApp"**

Instale o switch 3132Q-V e o painel de passagem em um gabinete NetApp , conforme necessário.

4. **"Revise o cabeamento e a configuração"**

Revise o suporte para portas Ethernet NVIDIA .

Instalar o switch de cluster 3132Q-V

Siga este procedimento para instalar e configurar o switch Cisco Nexus 3132Q-V.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões NX-os e Reference Configuration File (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.

- Concluído"fichas de trabalho de cablagem" .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- "Documentação necessária do switch e do ONTAP" .

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o…	Então…
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte o guia *Instalando um switch de cluster Cisco Nexus 3132Q-V e o painel pass-through em um gabinete NetApp* para obter instruções para instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.

O que se segue?

Opcionalmente, você pode"instalar um switch Cisco Nexus 3132Q-V em um gabinete NetApp" . Caso contrário, vá para"Revise o cabeamento e a configuração" .

Instale um switch de cluster Cisco Nexus 3132Q-V em um gabinete NetApp

Dependendo da sua configuração, você pode precisar instalar o switch Cisco Nexus 3132Q-V e o painel pass-through em um gabinete NetApp com os suportes padrão que estão incluídos no switch.

Antes de começar

- Os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança no "Guia de instalação de hardware do Cisco Nexus 3000 Series". Reveja estes documentos antes de iniciar o procedimento.
- O kit de painel de passagem, disponível na NetApp (código de peça X8784-R6). O kit do painel de passagem do NetApp contém o seguinte hardware:
  - Um painel obturador de passagem
  - Quatro parafusos 10-32 x .75
  - Quatro porcas de freio 10-32
- Oito parafusos 10-32 ou 12-24 e porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiros e traseiros do armário.
- Kit de trilho padrão Cisco para instalar o interrutor em um gabinete NetApp.

Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

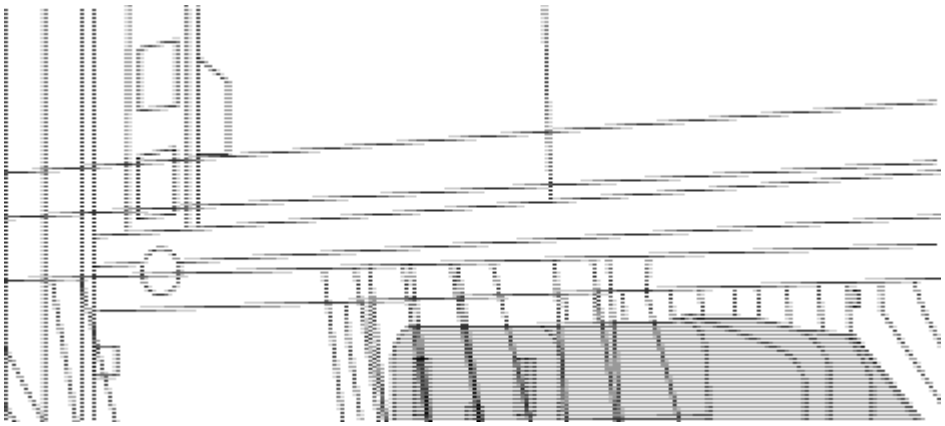
   a. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

      Neste procedimento, o painel obturador será instalado em U40.

   b. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

   c. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

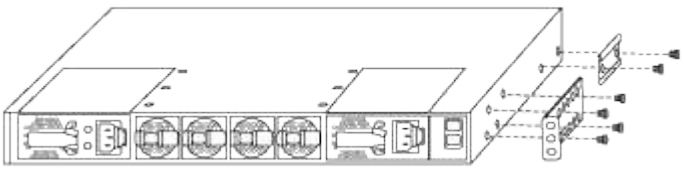
   d. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.



(1) conetor fêmea do cabo de ligação em ponte.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 3132Q-V.

   a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.

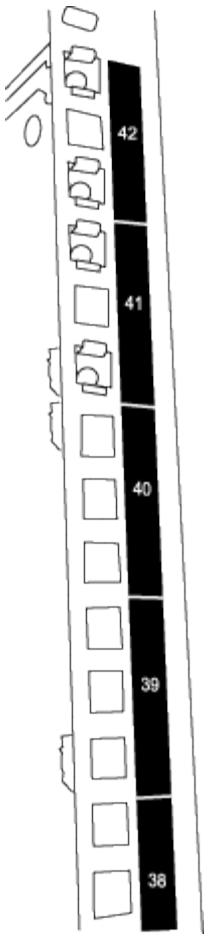


   b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.

   c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.

   d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.

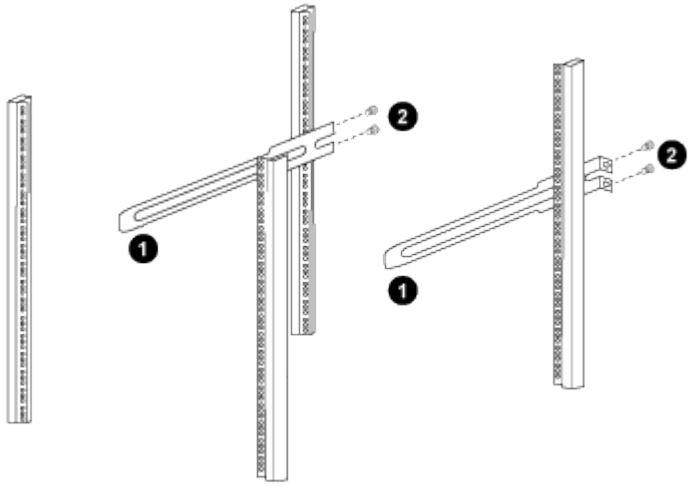
3. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



Os dois interrutores de 3132Q V serão sempre montados no topo 2U do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no gabinete.

   a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



(1) enquanto desliza suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.

(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

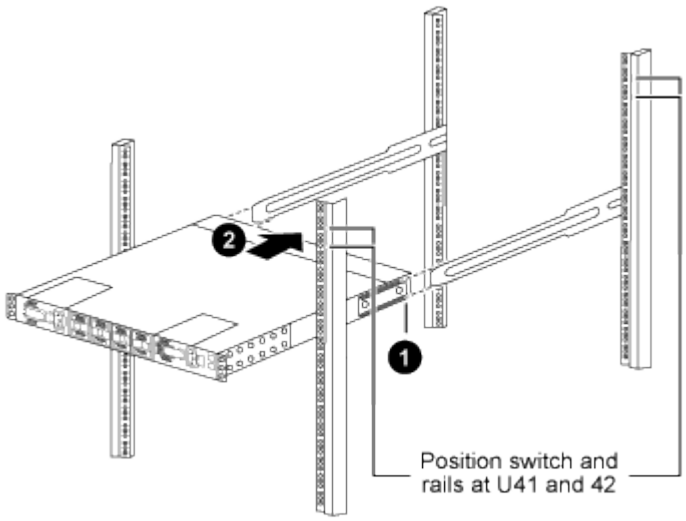
a. Repita o passo 4a para a coluna traseira do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

5. Instale o interrutor no gabinete.

> Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

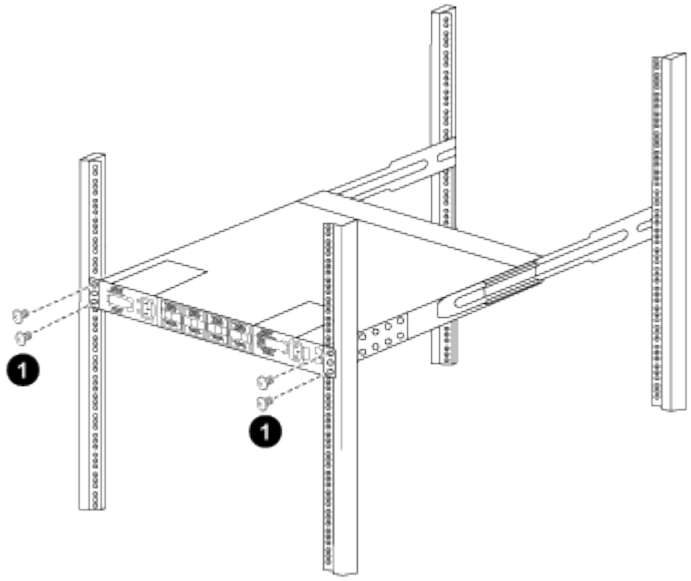
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo interrutor durante o processo de instalação.

6. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
7. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

8. Conete a porta de gerenciamento em cada switch de 3132Q V a um dos switches de gerenciamento (se solicitado) ou conete-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração

Antes de configurar seu switch Cisco 3132Q-V, revise as seguintes considerações.

Suporte para portas NVIDIA CX6, CX6-DX e CX7 Ethernet

Se estiver conetando uma porta de switch a um controlador ONTAP usando as portas de NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), é necessário codificar a velocidade da porta do switch.

```
(cs1)(config)# interface Ethernet1/19
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Configure o software

Fluxo de trabalho de instalação de software para switches de cluster Cisco Nexus 3132Q-V

Para instalar e configurar o software para um switch Cisco Nexus 3132Q-V e instalar ou atualizar o arquivo de configuração de referência (RCF), siga estas etapas:

1 **"Configure o interrutor"**

Configure o switch de cluster 3132Q-V.

2 **"Prepare-se para instalar o software NX-os e o RCF"**

O software Cisco NX-OS e o RCF devem ser instalados nos switches de cluster Cisco 3132Q-V.

3 **"Instale ou atualize o software NX-os"**

Baixe e instale ou atualize o software NX-OS no switch de cluster Cisco 3132Q-V.

4 **"Instale o RCF"**

Instale o RCF após configurar o switch Cisco 3132Q-V pela primeira vez.

5 **"Verifique a configuração do SSH"**

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

6 **"Redefinir o switch para os padrões de fábrica"**

Apague as configurações do switch do cluster 3132Q-V.

Configure o switch Cisco Nexus 3132Q-V.

Siga este procedimento para configurar o switch Cisco Nexus 3132Q-V.

Antes de começar

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões de NX-os e arquivo de configuração de referência (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Documentação necessária do switch de rede, documentação do controlador e documentação do ONTAP. Para obter mais informações, "Documentação necessária"consulte .
- Licenças aplicáveis, informações de rede e configuração e cabos.
- Fichas de trabalho de cablagem concluídas. "Folha de cálculo completa de cabeamento Cisco Nexus 3132Q-V."Consulte .
- RCFs de rede e de gerenciamento de cluster NetApp aplicáveis, baixados do site de suporte da NetApp em "mysupport.NetApp.com" para os switches que você recebe. Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o seu…	Então…
Cisco Nexus 3132Q-V em um gabinete de sistema NetApp	Consulte o guia *Instalando um switch de cluster Cisco Nexus 3132Q-V e o painel pass-through em um gabinete NetApp* para obter instruções para instalar o switch em um gabinete NetApp.
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster às controladoras usando a Planilha de cabeamento concluído, conforme descrito em "Folha de cálculo completa de cabeamento Cisco Nexus 3132Q-V.".
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.
4. Execute uma configuração inicial dos switches de rede do cluster.

   Forneça respostas aplicáveis às seguintes perguntas de configuração inicial ao inicializar o switch pela primeira vez. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Aviso	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com **sim**. A predefinição é não
Pretende aplicar o padrão de palavra-passe seguro? (sim/não)	Responda com **sim**. O padrão é sim.
Introduza a palavra-passe para admin:	A senha padrão é "'admin'"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Pretende introduzir a caixa de diálogo de configuração básica? (sim/não)	Responda com **sim** na configuração inicial do comutador.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em administradores alternativos. O padrão é **não**.
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com **não**. A predefinição é não
Configurar string de comunidade SNMP de leitura-escrita? (sim/não)	Responda com **não**. A predefinição é não
Introduza o nome do interrutor.	O nome do switch está limitado a 63 carateres alfanuméricos.

Aviso	Resposta
Continuar com a configuração de gerenciamento fora da banda (mgmt0)? (sim/não)	Responda com **yes** (o padrão) nesse prompt. No prompt mgmt0 IPv4 address:, insira seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com **sim**. No endereço IPv4 do prompt default-gateway:, digite seu default_gateway.
Configurar opções IP avançadas? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço telnet? (sim/não)	Responda com **não**. A predefinição é não
Ativar o serviço SSH? (sim/não)	Responda com **sim**. O padrão é sim. O SSH é recomendado ao usar o Ethernet Switch Health Monitor (CSHM) para seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Introduza o tipo de chave SSH que pretende gerar (dsa/rsa/rsa1).	O padrão é **rsa**.
Introduza o número de bits de chave (1024-2048).	Introduza os bits de chave de 1024-2048.
Configurar o servidor NTP? (sim/não)	Responda com **não**. A predefinição é não
Configurar a camada de interface padrão (L3/L2):	Responda com **L2**. A predefinição é L2.
Configurar o estado predefinido da interface da porta do switch (Shut/noshut):	Responda com **noshut**. O padrão é noshut.
Configurar o perfil do sistema CoPP (strict/moderate/lenient/dense):	Responda com **strict**. O padrão é rigoroso.
Pretende editar a configuração? (sim/não)	Você deve ver a nova configuração neste momento. Reveja e faça as alterações necessárias à configuração que acabou de introduzir. Responda com **no** no prompt se você estiver satisfeito com a configuração. Responda com **yes** se quiser editar as configurações.

Aviso	Resposta
Utilizar esta configuração e guardá-la? (sim/não)	Responda com **yes** para salvar a configuração. Isto atualiza automaticamente as imagens do Kickstart e do sistema. Se você não salvar a configuração nesta fase, nenhuma das alterações entrará em vigor na próxima vez que você reiniciar o switch.

5. Verifique as opções de configuração que você fez no visor que aparece no final da configuração e certifique-se de salvar a configuração.
6. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software suportada pelo NetApp para os switches a partir da "Transferência do software Cisco" página.

O que se segue?

"Prepare-se para instalar o NX-os e o RCF".

Prepare-se para instalar o software NX-os e o ficheiro de configuração de referência

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento usam dois nós. Esses nós usam duas portas de interconexão de cluster 10GbE `e0a` e `e0b`.

Consulte "Hardware Universe"para verificar as portas de cluster corretas nas suas plataformas.

As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `cluster1-01` e `cluster1-02`.
- Os nomes de LIF do cluster são `cluster1-01_clus1` e `cluster1-01_clus2` para cluster1-01 e `cluster1-02_clus1` e `cluster1-02_clus2` para cluster1-02.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde *x* é a duração da janela de manutenção em horas.

A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   network device-discovery show -protocol cdp
   ```

   Mostrar exemplo

   ```
   cluster1::*> network device-discovery show -protocol cdp

   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID)  Interface
   Platform
   ----------- ------ ------------------------- -----------------
   --------
   cluster1-02/cdp
               e0a    cs1                       Eth1/2            N3K-
   C3132Q-V
               e0b    cs2                       Eth1/2            N3K-
   C3132Q-V
   cluster1-01/cdp
               e0a    cs1                       Eth1/1            N3K-
   C3132Q-V
               e0b    cs2                       Eth1/1            N3K-
   C3132Q-V
   ```

4. Verifique o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede:

      ```
      network port show –ipspace Cluster
      ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy
```

b. Exibir informações sobre os LIFs:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o `auto-revert` comando está ativado em todas as LIFs do cluster:

`network interface show -vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
```

O que se segue?

"Instale o software NX-os".

Instale o software NX-os

Siga este procedimento para instalar o software NX-os no switch de cluster Nexus 3132Q-V.

Rever os requisitos

Antes de começar

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- "Switch Ethernet Cisco". Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.
- "Switches Cisco Nexus 3000 Series". Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

Instale o software

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Certifique-se de que conclui o procedimento em "Prepare-se para instalar o software NX-os e o ficheiro de configuração de referência"e, em seguida, siga os passos abaixo.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   ```
   cs2# ping 172.19.2.1 vrf management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

4. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão **up** com um status de integridade:

      `network port show -role cluster`

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -role Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

`system cluster-switch show -is-monitoring-enabled-operational true`

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desative a reversão automática nos LIFs do cluster. Os LIFs de cluster fazem failover para o switch de cluster do parceiro e permanecem lá enquanto você executa o procedimento de atualização no switch de destino:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Copie o software NX-os para o switch Nexus 3132Q-V usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para obter mais informações sobre comandos Cisco, consulte o guia apropriado no "Guias de referência de comando Cisco Nexus 3000 Series NX-os".

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password: xxxxxxxx
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
                NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
cs2#
```

8. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS


Compatibility check is done:
Module  bootable          Impact              Install-type  Reason
------- ----------------- ------------------- -------------
---------
     1     yes            Disruptive          Reset         Default
upgrade is not hitless


Images will be upgraded according to following table:
Module       Image       Running-Version(pri:alt)
New-Version          Upg-Required
------------ ----------- ----------------------------------------
-------------------- ------------
     1       nxos        9.3(3)
9.3(4)               yes
     1       bios        v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)   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.
cs2#
```

9. Verifique a nova versão do software NX-os depois que o switch reiniciar:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
NXOS: version 9.3(4)
  BIOS compile time:  05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]


Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

10. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

       ```
       network port show -role cluster
       ```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N3K-
```

```
C3132Q-V
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

11. Verifique se o cluster está em bom estado:

    `cluster show`

    Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

12. Repita os passos 6 a 11 no interrutor CS1.
13. Ative a reversão automática nos LIFs do cluster.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

14. Verifique se os LIFs do cluster reverteram para sua porta inicial:

```
network interface show -role cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Se qualquer LIFs de cluster não retornar às portas iniciais, reverta-as manualmente do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que se segue?

"Instalar o ficheiro de configuração de referência (RCF)".

Instalar ou atualizar o ficheiro de configuração de referência (RCF)

Siga este procedimento para instalar o RCF depois de configurar o interrutor Nexus 3132Q-V pela primeira vez. Você também pode usar este procedimento para atualizar sua versão RCF.

Rever os requisitos

Antes de começar

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O ficheiro de configuração de referência atual (RCF).
- É necessária uma ligação de consola ao interrutor ao instalar o RCF. Esse requisito é opcional se você tiver usado o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para limpar a configuração de antemão.
- "Switch Ethernet Cisco". Consulte a tabela de compatibilidade do switch para as versões ONTAP e RCF suportadas. Note que pode haver dependências de comando entre a sintaxe de comando no RCF e aquela encontrada em versões do NX-os.
- "Switches Cisco Nexus 3000 Series". Consulte os guias de software e atualização apropriados disponíveis no site da Cisco para obter a documentação completa sobre os procedimentos de atualização e downgrade do switch Cisco.

Instale o ficheiro

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `cluster1-01` `cluster1-02` , , `cluster1-03` `cluster1-04` e .
- Os nomes de LIF do cluster são `cluster1-01_clus1`, `cluster1-01_clus2` `cluster1-02_clus1` , `cluster1-02_clus2` , `cluster1-03_clus1`, , , `cluster1-03_clus2`, `cluster1-04_clus1`, e `cluster1-04_clus2`.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Certifique-se de que conclui o procedimento em "Prepare-se para instalar o software NX-os e o ficheiro de configuração de referência"e, em seguida, siga os passos abaixo.

Passo 1: Verifique o status da porta

1. Exiba as portas do cluster em cada nó conetado aos switches do cluster:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta de cluster.

   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:

      `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:

```
network interface show -vserver Cluster
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.0.0.1
NX3132QV
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.0.0.2
NX3132QV
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Para o ONTAP 9.8 e posterior, use o comando `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Desative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

Certifique-se de que a reversão automática esteja desativada após executar este comando.

4. No switch de cluster CS2, encerre as portas conetadas às portas de cluster dos nós.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit
```

O número de portas exibidas varia de acordo com o número de nós no cluster.

5. Verifique se as portas de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster`

   Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

6. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
cluster1::*>
```

Passo 2: Configure e verifique a configuração

1. Se você ainda não fez isso, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

   ```
   show running-config
   ```

2. Registre quaisquer adições personalizadas entre a configuração atual e o arquivo RCF em uso.
3. Salve os detalhes básicos da configuração em `write_erase.cfg` arquivo no bootflash.

   Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conectado à porta serial do console do switch para configurá-lo novamente.

   ```
   cs2# show run | section "switchname" > bootflash:write_erase.cfg

   cs2# show run | section "hostname" >> bootflash:write_erase.cfg

   cs2# show run | i "username admin password" >> bootflash:write_erase.cfg

   cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
   ```

4. Para RCF versão 1.12 e posteriores, execute os seguintes comandos:

   ```
   cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
   bootflash:write_erase.cfg

   cs2# echo "hardware access-list tcam region racl 256" >>
   bootflash:write_erase.cfg

   cs2# echo "hardware access-list tcam region e-racl 256" >>
   bootflash:write_erase.cfg
   ```

```
cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

Veja o artigo da Base de Conhecimento"Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota" para mais detalhes.

5. Verifique se o `write_erase.cfg` o arquivo é preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

6. Emitir o `write erase` comando para apagar a configuração salva atual:

```
cs2# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

7. Copie a configuração básica salva anteriormente na configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

8. Execute uma reinicialização do switch:

```
cs2# reload

This command will reboot the system. (y/n)? [n] y
```

9. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 3000 Series NX-os" guias.

Mostrar exemplo

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server......Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

10. Aplique o RCF baixado anteriormente ao flash de inicialização.

Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no"Referência de comando Cisco Nexus 3000 Series NX-os" guias.

Mostrar exemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

11. Examine a saída do banner a partir do `show banner motd` comando. Você deve ler e seguir as instruções em **Notas importantes** para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
cs2# show banner motd

*****************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Cisco Nexus 3132Q-V
* Filename : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : Nov-02-2020
* Version  : v1.6
*
* Port Usage : Breakout configuration
* Ports  1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports  7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```
* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*    - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*      NX-OS using a version later than 9.3(5).
*    - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*    - After the RCF is applied and switch rebooted, then proceed to
upgrade
*      NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*      after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*     hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*     hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*     hardware profile front portmode qsfp      (To reset to QSFP)
*
**********************************************************************
**********
```

12. Verifique se o arquivo RCF é a versão mais recente correta:

    `show running-config`

    Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

    - O banner RCF
    - As configurações de nó e porta
    - Personalizações

      A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

    > Para obter instruções sobre como colocar as portas 10GbE online após uma atualização do RCF, consulte o artigo da base de dados de Conhecimento "As portas de 10GbE GbE em um switch de cluster Cisco 3132Q não estão online" .

13. Depois de verificar se as versões do RCF e as configurações do switch estão corretas, copie o arquivo running-config para o arquivo startup-config.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Referência de comando Cisco Nexus 3000 Series NX-os" nos guias.

Mostrar exemplo

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

14. Interrutor de reinicialização CS2. Você pode ignorar os eventos "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado e a saída de erro `% Invalid command at '^' marker`.

Mostrar exemplo

```
cs2# reload
This command will reboot the system. (y/n)?  [n] y
```

15. Aplique o mesmo RCF e salve a configuração em execução pela segunda vez. Isso é necessário, já que o RCF utiliza QoS e requer reconfiguração TCAM que envolve o carregamento do RCF duas vezes com o switch reinicializado no meio.

Mostrar exemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

16. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
17. Verifique a integridade das portas de cluster no cluster.

    a. Verifique se as portas do cluster estão ativas e íntegras em todos os nós do cluster:

    ```
    network port show -ipspace Cluster
    ```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Verifique a integridade do switch a partir do cluster.

```
network device-discovery show -protocol cdp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7
N3K-C3132Q-V
            e0d    cs2                       Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8
N3K-C3132Q-V
            e0d    cs2                       Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1
N3K-C3132Q-V
            e0b    cs2                       Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2
N3K-C3132Q-V
            e0b    cs2                       Ethernet1/1/2
N3K-C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90
N3K-C3132Q-V
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
```

```
N3K-C3132Q-V
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Para o ONTAP 9.8 e posterior, use o comando `system switch ethernet show -is-monitoring-enabled-operational true`.

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF carregada anteriormente no switch:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

+

Pode levar até 5 minutos para que os nós de cluster relatem como íntegros.

18. No switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

Mostrar exemplo

```
cs1> enable
cs1# configure
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1# exit
```

O número de portas exibidas varia de acordo com o número de nós no cluster.

19. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch CS2. Isso pode levar alguns segundos.

    `network interface show -vserver Cluster`

    Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

20. Verifique se o cluster está em bom estado:

    `cluster show`

Mostrar exemplo

```
cluster1::*> cluster show
Node                  Health   Eligibility   Epsilon
--------------------- -------- ------------- -------
cluster1-01           true     true          false
cluster1-02           true     true          false
cluster1-03           true     true          true
cluster1-04           true     true          false
4 entries were displayed.
cluster1::*>
```

21. Repita os passos 1 a 17 no switch cs1.
22. Ative a reversão automática nos LIFs do cluster.

Mostrar exemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

23. Interrutor de reinicialização CS1. Você faz isso para acionar os LIFs do cluster para reverter para suas portas domésticas. Você pode ignorar os eventos "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
cs1# reload
This command will reboot the system. (y/n)?  [n] y
```

Etapa 3: Verifique a configuração

1. Verifique se as portas do switch conetadas às portas do cluster estão ativadas.

```
show interface brief | grep up
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

2. Verifique se o ISL entre CS1 e CS2 está funcional:

   `show port-channel summary`

Mostrar exemplo

```
cs1# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
cs1#
```

3. Verifique se os LIFs do cluster reverteram para sua porta inicial:

   `network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

4. Verifique se o cluster está em bom estado:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
cluster1::*>
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

O que se segue?

"Verifique a configuração do SSH".

Verifique a configuração da SSH

Se você estiver usando os recursos CSHM (Ethernet Switch Health Monitor) e coleta de logs, verifique se as chaves SSH e SSH estão habilitadas nos switches de cluster.

Passos

1. Verifique se o SSH está ativado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verifique se as chaves SSH estão ativadas:

```
show ssh key
```

Mostrar exemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Ao ativar o FIPS, você deve alterar o número de bits para 256 na central usando o comando `ssh key ecdsa 256 force`. "Configurar a segurança da rede usando o FIPS"Consulte para obter mais detalhes.

O que se segue?

"Configurar o monitoramento de integridade do switch".

Redefinir o switch do cluster 3132Q-V para os padrões de fábrica

Para redefinir o switch de cluster 3132Q-V para os padrões de fábrica, você deve apagar as configurações do switch 3132Q-V.

Sobre esta tarefa

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

Passos

1. Apagar a configuração existente:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Recarregue o software do switch:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   O sistema é reinicializado e entra no assistente de configuração. Durante a inicialização, se você receber o prompt “Abortar provisionamento automático e continuar com a configuração normal? (sim/não)[n]”, você deve responder **sim** para prosseguir.

Migrar switches

Migração de switch de CN1610 GbE

Migrar de switches CN1610 para o fluxo de trabalho dos switches Nexus 3132Q-V.

Siga estas etapas do fluxo de trabalho para migrar seus switches CN1610 para switches Cisco Nexus 3132Q-V.

1. **"Requisitos de migração"**

   Revise os requisitos e informações de exemplo do switch para o processo de migração.

2. **"Prepare-se para a migração"**

Prepare seus switches CN1610 para migração para os switches Nexus 3132Q-V.

3 **"Configure as portas"**

Configure suas portas para migração para os novos switches Nexus 3132Q-V.

4 **"Conclua a migração"**

Conclua a migração para os novos switches Nexus 3132Q-V.

Requisitos de migração

Os switches Cisco Nexus 3132Q-V podem ser usados como switches de cluster em seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Para obter mais informações, consulte:

- "Página de descrição do NetApp CN1601 e CN1610"
- "Página de descrição do comutador Ethernet Cisco"
- "Hardware Universe"

CN1610 requisitos

Os seguintes switches de cluster são suportados:

- NetApp CN1610
- Cisco Nexus 3132Q-V

Os switches do cluster suportam as seguintes conexões de nós:

- NetApp CN1610: Portas de 0/1 a 0/12 (10 GbE)
- Cisco Nexus 3132QP-V: Portas E1/1-30 (40/100 GbE)

Os interrutores do grupo de instrumentos utilizam as seguintes portas ISL (Inter-Switch Link):

- NetApp CN1610: Portas de 0/13 a 0/16 (10 GbE)
- Cisco Nexus 3132QP-V: Portas E1/31-32 (40/100 GbE)

O "Hardware Universe" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:

- Os nós com conexões de cluster de 10 GbE exigem cabos de conexões de fibra ótica QSFP para SFP ou cabos de conexões de cobre QSFP para SFP
- Os nós com conexões de cluster de 40/100 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ótica ou cabos de conexão direta de cobre QSFP/QSFP28

O cabeamento ISL apropriado é o seguinte:

- Início: Para CN1610 GbE a CN1610 GbE (SFP a SFP), quatro cabos de conexão direta de fibra ótica SFP ou cobre
- Interino: Para CN1610 para Nexus 3132Q-V (QSFP para quatro SFP mais breakout), um cabo de fibra ótica QSFP para SFP ou de cobre breakout
- Final: Para Nexus 3132Q-V para Nexus 3132Q-V (QSFP28 a QSFP28), dois cabos de fibra ótica QSFP28 ou cobre de ligação direta

Os cabos NetApp twinax não são compatíveis com os switches Cisco Nexus 3132Q-V.

Se a sua configuração atual do CN1610 utilizar cabos NetApp twinax para ligações de cluster-nó-a-switch ou ISL e pretender continuar a utilizar o twinax no seu ambiente, tem de adquirir cabos Cisco twinax. Como alternativa, você pode usar cabos de fibra ótica tanto para as conexões ISL quanto para as conexões cluster-node para switch.

Sobre os exemplos usados

Os exemplos neste procedimento descrevem a substituição de switches CN1610 por switches Cisco Nexus 3132Q-V. Pode utilizar estes passos (com modificações) para outras centrais Cisco mais antigas.

O procedimento também usa a seguinte nomenclatura de switch e nó:

- As saídas de comando podem variar dependendo de diferentes versões do ONTAP.
- Os CN1610 interrutores a substituir são **CL1** e **CL2**.
- Os switches Nexus 3132Q-V para substituir os switches CN1610 são **C1** e **C2**.
- **n1_clus1** é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- **n1_clus2** é o primeiro cluster LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus3** é o segundo LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus4** é o segundo LIF conetado ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- O número de portas 10 GbE e 40/100 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis na "Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" página.
- Os nós são **n1**, **n2**, **n3** e **n4**.

Os exemplos neste procedimento usam quatro nós:

- Dois nós usam quatro portas de interconexão de cluster de 10 GbE: **e0a**, **e0b**, **e0c** e **e0d**.
- Os outros dois nós usam duas portas de interconexão de cluster de 40 GbE: **e4a** e **e4e**.

  A "Hardware Universe" lista as portas de cluster reais em suas plataformas.

O que se segue?

"Prepare-se para a migração".

Prepare-se para a migração de switches CN1610 para switches 3132Q-V.

Siga estas etapas para preparar seus switches CN1610 para migração para switches Cisco Nexus 3132Q-V.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   ```
   network device-discovery show
   ```

   Mostrar exemplo

   O exemplo a seguir mostra quantas interfaces de interconexão de cluster foram configuradas em cada nó para cada switch de interconexão de cluster:

   ```
   cluster::> network device-discovery show

          Local  Discovered
   Node   Port   Device       Interface   Platform
   ------ ------ ------------ ----------- ----------
   n1     /cdp
           e0a   CL1          0/1         CN1610
           e0b   CL2          0/1         CN1610
           e0c   CL2          0/2         CN1610
           e0d   CL1          0/2         CN1610
   n2     /cdp
           e0a   CL1          0/3         CN1610
           e0b   CL2          0/3         CN1610
           e0c   CL2          0/4         CN1610
           e0d   CL1          0/4         CN1610

   8 entries were displayed.
   ```

3. Determine o status administrativo ou operacional de cada interface de cluster.

   a. Exibir os atributos da porta de rede do cluster:

      ```
      network port show
      ```

Mostrar exemplo

O exemplo a seguir exibe os atributos da porta de rede em um sistema:

```
cluster::*> network port show -role Cluster
       (network port show)

Node: n1
                 Broadcast               Speed (Mbps) Health Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

Node: n2
                 Broadcast               Speed (Mbps) Health Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

8 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas
`network interface show`

Mostrar exemplo

O exemplo a seguir exibe as informações gerais sobre todas as LIFs no sistema:

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true

8 entries were displayed.
```

c. Exibir informações sobre os switches de cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo a seguir exibe os switches de cluster que são conhecidos pelo cluster, juntamente com seus endereços IP de gerenciamento:

```
cluster::> system cluster-switch show

Switch                        Type             Address       Model
----------------------------- ---------------- -------------
--------
CL1                           cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

CL2                           cluster-network  10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

2 entries were displayed.
```

4. Defina `-auto-revert` o parâmetro como false em LIFs de cluster clus1 e clus4 em ambos os nós:

   `network interface modify`

Mostrar exemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert false
```

5. Verifique se o RCF e a imagem apropriados estão instalados nos novos switches 3132Q-V conforme necessário para seus requisitos e faça qualquer personalização essencial do site, como usuários e senhas, endereços de rede, etc.

Neste momento, tem de preparar ambos os interrutores. Se você precisar atualizar o RCF e a imagem, siga estas etapas:

a. Ver"Switches Ethernet Cisco" no site de suporte da NetApp .
b. Observe o switch e as versões de software necessárias na tabela nessa página.
c. Baixe a versão apropriada do RCF.
d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
e. Transfira a versão apropriada do software de imagem.

   "Download do arquivo de configuração de referência do comutador de rede de gerenciamento e cluster Cisco"

6. Migrar os LIFs associados ao segundo switch CN1610 a ser substituído:

```
network interface migrate
```

> É necessário migrar as LIFs de cluster de uma conexão para o nó, seja por meio do processador de serviços ou da interface de gerenciamento de nós, que possui o LIF do cluster que está sendo migrado.

Mostrar exemplo

O exemplo a seguir mostra n1 e n2, mas a migração de LIF deve ser feita em todos os nós:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-destination-node  n1  -destination-port  e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-destination-node  n1  -destination-port  e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-destination-node  n2  -destination-port  e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-destination-node  n2  -destination-port  e0d
```

7. Verifique a integridade do cluster:

```
network interface show
```

Mostrar exemplo

O exemplo a seguir mostra o resultado do comando anterior `network interface migrate`:

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network         Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask    Node     Port
Home
-------- ---------- ----------- --------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24    n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24    n1       e0a
false
         n1_clus3   up/up       10.10.0.3/24    n1       e0d
false
         n1_clus4   up/up       10.10.0.4/24    n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24    n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24    n2       e0a
false
         n2_clus3   up/up       10.10.0.7/24    n2       e0d
false
         n2_clus4   up/up       10.10.0.8/24    n2       e0d
true

8 entries were displayed.
```

8. Encerre as portas de interconexão de cluster que estão fisicamente conetadas ao switch CL2:

   `network port modify`

Mostrar exemplo

Os comandos a seguir desligam as portas especificadas no n1 e no n2, mas as portas devem ser fechadas em todos os nós:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source      Destination   Packet
Node   Date                       LIF         LIF           Loss
------ -------------------------- ---------- -------------- -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n1_clus1       none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2       none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1       none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2       none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. encerre as portas ISL 13 a 16 no interrutor CN1610 ativo CL1:

```
shutdown
```

Mostrar exemplo

O exemplo a seguir mostra como desligar as portas ISL 13 a 16 no switch CN1610 CL1:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16
(CL1)(Interface 0/13-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

2. Construa um ISL temporário entre CL1 e C2:

Mostrar exemplo

O exemplo a seguir cria um ISL temporário entre CL1 (portas 13-16) e C2 (portas E1/24/1-4):

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

O que se segue?

"Configure as portas".

Configure suas portas para migração de switches CN1610 para switches 3132Q-V.

Siga estas etapas para configurar suas portas para migração dos switches CN1610 para os novos switches Nexus 3132Q-V.

Passos

1. Em todos os nós, remova os cabos que estão conetados ao switch CN1610 CL2.

   Com o cabeamento compatível, você precisa reconetar as portas desconetadas em todos os nós ao switch Nexus 3132Q-V C2.

2. Remova quatro cabos ISL das portas 13 a 16 no interrutor CN1610 CL1.

   Você deve conetar o Cisco QSFP apropriado aos cabos de conexão da porta 1/24 no novo switch Cisco 3132Q-V C2, às portas 13 a 16 no switch CN1610 existente CL1.

   > Ao reconetar quaisquer cabos ao novo switch Cisco 3132Q-V, você deve usar cabos de fibra ótica ou Cisco twinax.

3. Para tornar o ISL dinâmico, configure a interface ISL 3/1 no interrutor CN1610 ativo para desativar o modo estático: `no port-channel static`

   Esta configuração corresponde à configuração ISL no interrutor 3132Q-V C2 quando os ISLs são apresentados em ambos os interrutores no passo 11.

   Mostrar exemplo

   O exemplo a seguir mostra a configuração da interface ISL 3/1 usando o `no port-channel static` comando para tornar o ISL dinâmico:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 3/1
   (CL1)(Interface 3/1)# no port-channel static
   (CL1)(Interface 3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

4. Abra ISLs 13 a 16 no interrutor CN1610 ativo CL1.

   Mostrar exemplo

   O exemplo a seguir ilustra o processo de criação das portas ISL 13 a 16 na interface de canal de porta 3/1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 0/13-0/16,3/1
   (CL1)(Interface 0/13-0/16,3/1)# no shutdown
   (CL1)(Interface 0/13-0/16,3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

5. Verifique se as ISLs estão `up` no interrutor CN1610 CL1:

   `show port-channel`

   O "Estado da ligação" deve ser `Up`, "tipo" deve ser `Dynamic`, e a coluna "porta ativa" deve ser `True` para as portas 0/13 a 0/16:

Mostrar exemplo

```
(CL1)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Dynamic
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port         Port
Ports  Timeout       Speed        Active
------ ------------- ----------   -------
0/13   actor/long    10 Gb Full   True
       partner/long
0/14   actor/long    10 Gb Full   True
       partner/long
0/15   actor/long    10 Gb Full   True
       partner/long
0/16   actor/long    10 Gb Full   True
       partner/long
```

6. Verifique se as ISLs estão `up` no interrutor 3132Q-V C2:

   `show port-channel summary`

Mostrar exemplo

As portas eth1/24/1 a eth1/24/4 devem indicar `(P)`, o que significa que todas as quatro portas ISL estão ativas no canal de porta. eth1/31 e eth1/32 devem indicar `(D)` uma vez que não estão ligados:

```
C2# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
----------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
----------
1     Po1(SU)     Eth      LACP      Eth1/31(D)   Eth1/32(D)
2     Po2(SU)     Eth      LACP      Eth1/24/1(P) Eth1/24/2(P)
Eth1/24/3(P)
                                     Eth1/24/4(P)
```

7. Abra todas as portas de interconexão de cluster que estão conetadas ao switch 3132Q-V C2 em todos os nós:

   `network port modify`

Mostrar exemplo

O exemplo a seguir mostra como abrir as portas de interconexão de cluster conetadas ao switch 3132Q-V C2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

8. Reverter todas as LIFs de interconexão de cluster migradas que estão conetadas ao C2 em todos os nós:

   `network interface revert`

Mostrar exemplo

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Verifique se todas as portas de interconexão de cluster são revertidas para suas portas iniciais:

   `network interface show`

Mostrar exemplo

O exemplo a seguir mostra que os LIFs no clus2 são revertidos para suas portas residenciais e mostra que os LIFs são revertidos com sucesso se as portas na coluna "porta atual" tiverem um status de `true` na coluna "está Início". Se o valor for Home for `false`, o LIF não será revertido.

```
cluster::*> network interface show -role cluster
       (network interface show)

         Logical    Status      Network         Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask    Node     Port
Home
-------- ---------- ----------- --------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24    n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24    n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24    n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24    n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24    n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24    n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24    n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24    n2       e0d
true

8 entries were displayed.
```

10. Verifique se todas as portas do cluster estão conetadas:

    `network port show`

Mostrar exemplo

O exemplo a seguir mostra o resultado do comando anterior `network port modify`, verificando se todas as interconexões de cluster são `up`:

```
cluster::*> network port show -role Cluster
       (network port show)

Node: n1
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain      Link  MTU   Admin/Open   Status   Health
Status
----- --------- ----------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster     up    9000  auto/10000     -        -
e0b   cluster   cluster     up    9000  auto/10000     -        -
e0c   cluster   cluster     up    9000  auto/10000     -        -
e0d   cluster   cluster     up    9000  auto/10000     -        -

Node: n2
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain      Link  MTU   Admin/Open   Status   Health
Status
----- --------- ----------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster     up    9000  auto/10000     -        -
e0b   cluster   cluster     up    9000  auto/10000     -        -
e0c   cluster   cluster     up    9000  auto/10000     -        -
e0d   cluster   cluster     up    9000  auto/10000     -        -

8 entries were displayed.
```

11. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source      Destination   Packet
Node   Date                       LIF         LIF           Loss
------ -------------------------- ---------- -------------- -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n1_clus1       none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2       none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1       none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2       none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. em cada nó no cluster, migre as interfaces associadas ao primeiro switch CN1610 CL1, para serem substituídas:

```
network interface migrate
```

Mostrar exemplo

O exemplo a seguir mostra as portas ou LIFs que estão sendo migradas nos nós n1 e n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-destination-node n2 -destination-port e0c
```

2. Verifique o status do cluster:

```
network interface show
```

Mostrar exemplo

O exemplo a seguir mostra que as LIFs de cluster necessárias foram migradas para as portas de cluster apropriadas hospedadas no switch de cluster C2:

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network        Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0b
false
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0c
false
         n2_clus1   up/up       10.10.0.5/24   n2       e0b
false
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0c
false

8 entries were displayed.
```

3. Encerre as portas de nós que estão conetadas ao CL1 em todos os nós:

   `network port modify`

Mostrar exemplo

O exemplo a seguir mostra como desligar as portas especificadas nos nós n1 e n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

4. Desligue as portas ISL 24, 31 e 32 no interrutor C2 ativo de 3132Q V:

   `shutdown`

   Mostrar exemplo

   O exemplo a seguir mostra como desligar ISLs 24, 31 e 32 no interrutor C2 ativo de 3132Q V:

   ```
   C2# configure
   C2(config)# interface ethernet 1/24/1-4
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# interface ethernet 1/31-32
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# exit
   C2#
   ```

5. Remova os cabos que estão conetados ao switch CN1610 CL1 em todos os nós.

   Com o cabeamento compatível, você precisa reconetar as portas desconetadas em todos os nós ao switch Nexus 3132Q-V C1.

6. Remova os cabos QSFP da porta E1/24 do Nexus 3132Q-V C2.

   Você deve conetar as portas E1/31 e E1/32 no C1 às portas E1/31 e E1/32 no C2 usando fibra ótica Cisco QSFP suportada ou cabos de conexão direta.

7. Restaure a configuração na porta 24 e remova o canal de porta temporário 2 no C2, copiando o `running-configuration` arquivo para `startup-configuration` o arquivo.

Mostrar exemplo

O exemplo a seguir copia o `running-configuration` arquivo para o `startup-configuration` arquivo:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

8. Abra as portas ISL 31 e 32 no C2, o interrutor ativo de 3132Q V:

`no shutdown`

Mostrar exemplo

O exemplo a seguir mostra como abrir ISLs 31 e 32 no interrutor 3132Q-V C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

O que se segue?

"Conclua a migração".

Conclua a sua migração de switches CN1610 para switches Nexus 3132Q-V.

Conclua as etapas a seguir para finalizar a migração de switches CN1610 para switches Nexus 3132Q-V.

Passos

1. Verifique se as conexões ISL estão `up` no interrutor 3132Q-V C2:

   `show port-channel summary`

   As portas eth1/31 e eth1/32 devem indicar `(P)`, o que significa que ambas as portas ISL estão `up` no canal de porta.

   Mostrar exemplo

   ```
   C1# show port-channel summary
   Flags:  D - Down        P - Up in port-channel (members)
           I - Individual  H - Hot-standby (LACP only)
           s - Suspended   r - Module-removed
           S - Switched    R - Routed
           U - Up (port-channel)
           M - Not in use. Min-links not met
   ------------------------------------------------------------------------
   ----------
   Group Port-       Type     Protocol  Member Ports
         Channel
   ------------------------------------------------------------------------
   ----------
   1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
   ```

2. Abra todas as portas de interconexão de cluster conetadas ao novo switch de 3132Q V C1 em todos os nós:

   `network port modify`

   Mostrar exemplo

   O exemplo a seguir mostra como abrir todas as portas de interconexão de cluster conetadas ao novo switch de 3132Q V C1:

   ```
   cluster::*> network port modify -node n1 -port e0a -up-admin true
   cluster::*> network port modify -node n1 -port e0d -up-admin true
   cluster::*> network port modify -node n2 -port e0a -up-admin true
   cluster::*> network port modify -node n2 -port e0d -up-admin true
   ```

3. Verifique o status da porta do nó do cluster:

   `network port show`

Mostrar exemplo

O exemplo a seguir verifica se todas as portas de interconexão de cluster no n1 e n2 no novo switch de 3132Q V C1 são `up`:

```
cluster::*> network port show -role Cluster
       (network port show)

Node: n1
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

Node: n2
                 Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace    Domain     Link  MTU    Admin/Open   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

8 entries were displayed.
```

4. Reverter todas as LIFs de interconexão de cluster migradas originalmente conetadas ao C1 em todos os nós:

   `network interface revert`

Mostrar exemplo

O exemplo a seguir mostra como reverter as LIFs de cluster migradas para suas portas iniciais:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Verifique se a interface está agora em casa:

   `network interface show`

Mostrar exemplo

O exemplo a seguir mostra o status das interfaces de interconexão de cluster é `up` e `Is home` para n1 e n2:

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network        Current  Current  Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true

8 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source      Destination   Packet
Node   Date                       LIF         LIF           Loss
------ -------------------------- ----------- ------------- -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2    n1_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2    n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2    n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2    n1_clus2      none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. expanda o cluster adicionando nós aos switches de cluster Nexus 3132Q-V.
2. Exiba as informações sobre os dispositivos em sua configuração:

- network device-discovery show
- network port show -role cluster
- network interface show -role cluster
- system cluster-switch show

Mostrar exemplo

Os exemplos a seguir mostram os nós n3 e n4 com portas de cluster de 40 GbE conetadas às portas E1/7 e E1/8, respetivamente nos switches de cluster Nexus 3132Q-V e ambos os nós aderiram ao cluster. As portas de interconexão de cluster de 40 GbE usadas são e4a e e4e.

```
cluster::*> network device-discovery show

       Local  Discovered
Node   Port   Device       Interface       Platform
------ ------ ------------ --------------- -------------
n1     /cdp
        e0a   C1           Ethernet1/1/1   N3K-C3132Q-V
        e0b   C2           Ethernet1/1/1   N3K-C3132Q-V
        e0c   C2           Ethernet1/1/2   N3K-C3132Q-V
        e0d   C1           Ethernet1/1/2   N3K-C3132Q-V
n2     /cdp
        e0a   C1           Ethernet1/1/3   N3K-C3132Q-V
        e0b   C2           Ethernet1/1/3   N3K-C3132Q-V
        e0c   C2           Ethernet1/1/4   N3K-C3132Q-V
        e0d   C1           Ethernet1/1/4   N3K-C3132Q-V
n3     /cdp
        e4a   C1           Ethernet1/7     N3K-C3132Q-V
        e4e   C2           Ethernet1/7     N3K-C3132Q-V
n4     /cdp
        e4a   C1           Ethernet1/8     N3K-C3132Q-V
        e4e   C2           Ethernet1/8     N3K-C3132Q-V

12 entries were displayed.
```

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1
                 Broadcast              Speed (Mbps) Health
Ignore
Port   IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a    cluster   cluster    up    9000  auto/10000     -        -
e0b    cluster   cluster    up    9000  auto/10000     -        -
e0c    cluster   cluster    up    9000  auto/10000     -        -
e0d    cluster   cluster    up    9000  auto/10000     -        -
```

```
Node: n2
                 Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

Node: n3
                 Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -        -
e4e   cluster   cluster    up    9000  auto/40000     -        -

Node: n4
                 Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -        -
e4e   cluster   cluster    up    9000  auto/40000     -        -

12 entries were displayed.
```

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true
         n3_clus1   up/up       10.10.0.9/24   n3       e4a
true
         n3_clus2   up/up       10.10.0.10/24  n3       e4e
true
         n4_clus1   up/up       10.10.0.11/24  n4       e4a
true
         n4_clus2   up/up       10.10.0.12/24  n4       e4e
true

12 entries were displayed.
```

```
cluster::> system cluster-switch show

Switch                      Type              Address       Model
--------------------------- ----------------- -------------
---------
C1                          cluster-network  10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network  10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                         cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

CL2                         cluster-network  10.10.1.102
CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

4 entries were displayed.
```

3. Extrair os CN1610 interrutores substituídos, se não forem removidos automaticamente:

   `system cluster-switch delete`

Mostrar exemplo

O exemplo a seguir mostra como remover os CN1610 switches:

```
cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2
```

4. Configure os clusters clus1 e clus4 para `-auto-revert` em cada nó e confirme:

Mostrar exemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert true
```

5. Verifique se os switches de cluster adequados são monitorados:

```
system cluster-switch show
```

Mostrar exemplo

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network    10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

6. se você suprimiu a criação automática de caso, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migração de switch Cisco Nexus 5596

Migrar de switches Nexus 5596 para o fluxo de trabalho dos switches Nexus 3132Q-V.

Siga estas etapas do fluxo de trabalho para migrar seus switches Cisco Nexus 5596 para switches Cisco Nexus 3132Q-V.

1 **"Requisitos de migração"**

Revise os requisitos e informações de exemplo do switch para o processo de migração.

2 **"Prepare-se para a migração"**

Prepare seus switches Nexus 5596 para migração para os switches Nexus 3132Q-V.

3 **"Configure as portas"**

Configure suas portas para migração para os novos switches Nexus 3132Q-V.

4 **"Conclua a migração"**

Conclua a migração para os novos switches Nexus 3132Q-V.

Requisitos de migração

Os switches Cisco Nexus 3132Q-V podem ser usados como switches de cluster em seu cluster AFF ou FAS. Os switches de cluster permitem que você crie clusters do ONTAP com mais de dois nós.

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Para obter mais informações, consulte:

- "Switch Ethernet Cisco"
- "Hardware Universe"

Cisco Nexus 5596 requisitos

Os switches de cluster usam as seguintes portas para conexões com nós:

- Nexus 5596: Portas E1/1-40 (10 GbE)
- Nexus 3132Q-V: Portas E1/1-30 (10/40/100 GbE)

Os switches do cluster usam as seguintes portas ISL (Inter-Switch Link):

- Nexus 5596: Portas E1/41-48 (10 GbE)
- Nexus 3132Q-V: Portas E1/31-32 (40/100 GbE)

O "*Hardware Universe*" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:

- Os nós com conexões de cluster de 10 GbE exigem cabos de conexões de fibra ótica QSFP para SFP ou cabos de conexões de cobre QSFP para SFP.
- Os nós com conexões de cluster de 40/100 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.

Os switches de cluster usam o cabeamento ISL apropriado:

- Início: Nexus 5596 (SFP para SFP)
  - 8x cabos de conexão direta de fibra ou cobre SFP
- Interino: Nexus 5596 para Nexus 3132Q-V (QSFP para mais de 4xSFP break-out)
  - 1x cabos de rutura de fibra QSFP para SFP ou de rutura de cobre
- Final: Nexus 3132Q-V para Nexus 3132Q-V (QSFP28 a QSFP28)
  - 2x QSFP28 cabos de ligação direta de fibra ou cobre
- Nos switches Nexus 3132Q-V, você pode operar portas QSFP/QSFP28 nos modos 40/100 Gigabit Ethernet ou 4 x10 Gigabit Ethernet.

  Por padrão, existem 32 portas no modo 40/100 Gigabit Ethernet. Essas 40 portas Gigabit Ethernet são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta 40 Gigabit Ethernet é numerada como 1/2.

  O processo de alteração da configuração de 40 Gigabit Ethernet para 10 Gigabit Ethernet é chamado *breakout* e o processo de alteração da configuração de 10 Gigabit Ethernet para 40 Gigabit Ethernet é chamado *breakin*.

  Quando você divide uma porta Ethernet de 40/100 Gigabit em 10 portas Gigabit Ethernet, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta 40/100 Gigabit Ethernet são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.
- No lado esquerdo dos switches Nexus 3132Q-V estão 2 portas SFP mais, chamadas 1/33 e 1/34.
- Você configurou algumas das portas nos switches Nexus 3132Q-V para serem executadas a 10 GbE ou 40/100 GbE.

  > Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP a partir da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.
- Você fez o Planejamento, a migração e leu a documentação necessária sobre a conectividade de 10 GbE e 40/100 GbE dos nós para os switches de cluster Nexus 3132Q-V.
- As versões do ONTAP e do NX-OS suportadas neste procedimento estão aqui:"Switches Ethernet Cisco" .

Sobre os exemplos usados

Os exemplos neste procedimento descrevem a substituição de switches Cisco Nexus 5596 por switches Cisco Nexus 3132Q-V. Pode utilizar estes passos (com modificações) para outras centrais Cisco mais antigas.

O procedimento também usa a seguinte nomenclatura de switch e nó:

- As saídas de comando podem variar dependendo de diferentes versões do ONTAP.
- Os switches Nexus 5596 a serem substituídos são **CL1** e **CL2**.
- Os switches Nexus 3132Q-V para substituir os switches Nexus 5596 são **C1** e **C2**.
- **n1_clus1** é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- **n1_clus2** é o primeiro cluster LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.

- **n1_clus3** é o segundo LIF conetado ao switch de cluster 2 (CL2 ou C2) para o nó **n1**.
- **n1_clus4** é o segundo LIF conetado ao switch de cluster 1 (CL1 ou C1) para o nó **n1**.
- O número de portas 10 GbE e 40/100 GbE são definidos nos arquivos de configuração de referência (RCFs) disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .
- Os nós são **n1**, **n2**, **n3** e **n4**.

Os exemplos neste procedimento usam quatro nós:

- Dois nós usam quatro portas de interconexão de cluster de 10 GbE: **e0a**, **e0b**, **e0c** e **e0d**.
- Os outros dois nós usam duas portas de interconexão de cluster de 40 GbE: **e4a** e **e4e**.

  A "*Hardware Universe*" lista as portas de cluster reais em suas plataformas.

Cenários abordados

Este procedimento abrange os seguintes cenários:

- O cluster começa com dois nós conectados e funcionando em dois switches de cluster Nexus 5596.
- O interrutor do cluster CL2 a ser substituído por C2 (passos 1 a 19):
  - O tráfego em todas as portas de cluster e LIFs em todos os nós conectados ao CL2 é migrado para as primeiras portas de cluster e LIFs conetadas ao CL1.
  - Desconete o cabeamento de todas as portas de cluster em todos os nós conectados ao CL2 e use o cabeamento de saída compatível para reconetar as portas ao novo switch de cluster C2.
  - Desconete o cabeamento entre as portas ISL entre CL1 e CL2 e, em seguida, use o cabeamento de saída suportado para reconetar as portas de CL1 a C2.
  - O tráfego em todas as portas de cluster e LIFs conetadas ao C2 em todos os nós é revertido.
- O interrutor do cluster CL2 a ser substituído por C2.
  - O tráfego em todas as portas de cluster ou LIFs em todos os nós conectados ao CL1 é migrado para as segundas portas de cluster ou LIFs conetadas ao C2.
  - Desconete o cabeamento de todas as portas de cluster em todos os nós conectados ao CL1 e reconete, usando o cabeamento de saída compatível, ao novo switch de cluster C1.
  - Desconete o cabeamento entre as portas ISL entre CL1 e C2 e reconete usando o cabeamento suportado, de C1 a C2.
  - O tráfego em todas as portas de cluster ou LIFs conetadas ao C1 em todos os nós é revertido.
- Dois nós de FAS9000 foram adicionados ao cluster com exemplos mostrando detalhes do cluster.

O que se segue?

"Prepare-se para a migração".

Prepare-se para a migração de switches Nexus 5596 para switches Nexus 3132Q-V.

Siga estas etapas para preparar seus switches Cisco Nexus 5596 para migração para switches Cisco Nexus 3132Q-V.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma

mensagem AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

x é a duração da janela de manutenção em horas.

> A mensagem notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   `network device-discovery show`

   Mostrar exemplo

   O exemplo a seguir mostra quantas interfaces de interconexão de cluster foram configuradas em cada nó para cada switch de interconexão de cluster:

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    CL1                Ethernet1/1      N5K-C5596UP
            e0b    CL2                Ethernet1/1      N5K-C5596UP
            e0c    CL2                Ethernet1/2      N5K-C5596UP
            e0d    CL1                Ethernet1/2      N5K-C5596UP
n2         /cdp
            e0a    CL1                Ethernet1/3      N5K-C5596UP
            e0b    CL2                Ethernet1/3      N5K-C5596UP
            e0c    CL2                Ethernet1/4      N5K-C5596UP
            e0d    CL1                Ethernet1/4      N5K-C5596UP
8 entries were displayed.
```

3. Determine o status administrativo ou operacional de cada interface de cluster:

   a. Exibir os atributos da porta de rede:

      `network port show`

Mostrar exemplo

O exemplo a seguir exibe os atributos da porta de rede em um sistema:

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

a. Exibir informações sobre as interfaces lógicas
`network interface show`

Mostrar exemplo

O exemplo a seguir exibe as informações gerais sobre todas as LIFs no sistema:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------ ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

b. Exibir informações sobre os switches de cluster descobertos
`system cluster-switch show`

Mostrar exemplo

O exemplo a seguir exibe os switches de cluster que são conhecidos pelo cluster, juntamente com seus endereços IP de gerenciamento:

```
cluster::*> system cluster-switch show

Switch                        Type               Address
Model
------------------------------ ------------------ ---------------
---------------
CL1                           cluster-network    10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP

2 entries were displayed.
```

4. Defina o `-auto-revert` parâmetro como `false` no cluster LIFs clus1 e clus2 em ambos os nós:

   `network interface modify`

Mostrar exemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

5. Verifique se o RCF e a imagem apropriados estão instalados nos novos switches 3132Q-V conforme necessário para seus requisitos e faça as personalizações essenciais do site, como usuários e senhas, endereços de rede, etc.

   Neste momento, tem de preparar ambos os interrutores. Se você precisar atualizar o RCF e a imagem, siga estas etapas:

   a. Vá para"Switches Ethernet Cisco" no site de suporte da NetApp .
   b. Observe o switch e as versões de software necessárias na tabela nessa página.
   c. Baixe a versão apropriada do RCF.
   d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
   e. Transfira a versão apropriada do software de imagem.

      Consulte a página *ONTAP 8.x ou mais recente Cluster and Management Network Switch Reference Configuration Files*Download e, em seguida, selecione a versão apropriada.

   Para encontrar a versão correta, consulte a página de download do comutador de rede de cluster *ONTAP 8.x ou posterior*.

6. Migrar os LIFs associados ao segundo switch Nexus 5596 a ser substituído:

   ```
   network interface migrate
   ```

Mostrar exemplo

O exemplo a seguir mostra n1 e n2, mas a migração de LIF deve ser feita em todos os nós:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

7. Verifique a integridade do cluster:

   `network interface show`

Mostrar exemplo

O exemplo a seguir mostra o resultado do comando anterior `network interface migrate`:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0a     false
            n1_clus3   up/up      10.10.0.3/24       n1
e0d     false
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0a     false
            n2_clus3   up/up      10.10.0.7/24       n2
e0d     false
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

8. Encerre as portas de interconexão de cluster que estão fisicamente conetadas ao switch CL2:

   `network port modify`

Mostrar exemplo

Os comandos a seguir desligam as portas especificadas no n1 e no n2, mas as portas devem ser fechadas em todos os nós:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------  -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2_clus1       none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2       none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1       none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2       none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. desligue as portas ISL de 41 a 48 no switch Nexus 5596 ativo CL1:

Mostrar exemplo

O exemplo a seguir mostra como desligar as portas ISL 41 a 48 no switch Nexus 5596 CL1:

```
(CL1)# configure
(CL1)(Config)# interface e1/41-48
(CL1)(config-if-range)# shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

Se você estiver substituindo um Nexus 5010 ou 5020, especifique os números de porta apropriados para o ISL.

2. Construa um ISL temporário entre CL1 e C2.

Mostrar exemplo

O exemplo a seguir mostra uma ISL temporária sendo configurada entre CL1 e C2:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

O que se segue?

"Configure as portas".

Configure suas portas para migração de switches 5596 para switches 3132Q-V.

Siga estas etapas para configurar suas portas para migração dos switches Nexus 5596 para os novos switches Nexus 3132Q-V.

Passos

1. Em todos os nós, remova todos os cabos conetados ao switch Nexus 5596 CL2.

   Com o cabeamento compatível, reconecte as portas desconetadas em todos os nós ao switch Nexus

3132Q-V C2.

2. Remova todos os cabos do switch Nexus 5596 CL2.

   Conete o Cisco QSFP apropriado aos cabos de conexão Ethernet 1/24 no novo switch Cisco 3132Q-V, C2, às portas 45 a 48 no Nexus 5596, CL1 existente.

3. Verifique se as interfaces eth1/45-48 já têm `channel-group 1 mode active` em sua configuração em execução.
4. Abra as portas ISLs 45 a 48 no switch Nexus 5596 ativo CL1.

   Mostrar exemplo

   O exemplo a seguir mostra que as portas ISLs 45 a 48 estão sendo criadas:

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/45-48
   (CL1)(config-if-range)# no shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

5. Verifique se os ISLs estão `up` no switch Nexus 5596 CL1:

   ```
   show port-channel summary
   ```

Mostrar exemplo

As portas eth1/45 a eth1/48 devem indicar (P), o que significa que as portas ISL `up` estão no canal de porta:

```
Example
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/41(D)   Eth1/42(D)
Eth1/43(D)
                                   Eth1/44(D)   Eth1/45(P)
Eth1/46(P)
                                   Eth1/47(P)   Eth1/48(P)
```

6. Verifique se as ISLs estão `up` no interrutor 3132Q-V C2:

   `show port-channel summary`

Mostrar exemplo

As portas eth1/24/1, eth1/24/2, eth1/24/3 e eth1/24/4 devem indicar (P) o que significa que as portas ISL `up` estão no canal de porta:

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(D)   Eth1/32(D)
2     Po2(SU)      Eth    LACP      Eth1/24/1(P)  Eth1/24/2(P)
Eth1/24/3(P)
                                   Eth1/24/4(P)
```

7. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao switch 3132Q-V C2:

   `network port modify`

   Mostrar exemplo

   O exemplo a seguir mostra as portas especificadas sendo criadas nos nós n1 e n2:

   ```
   cluster::*> network port modify -node n1 -port e0b -up-admin true
   cluster::*> network port modify -node n1 -port e0c -up-admin true
   cluster::*> network port modify -node n2 -port e0b -up-admin true
   cluster::*> network port modify -node n2 -port e0c -up-admin true
   ```

8. Em todos os nós, reverta todas as LIFs de interconexão de cluster migradas conetadas ao C2:

   `network interface revert`

Mostrar exemplo

O exemplo a seguir mostra as LIFs de cluster migradas sendo revertidas para suas portas residenciais nos nós n1 e n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Verifique se todas as portas de interconexão de cluster estão agora revertidas para sua casa:

   `network interface show`

Mostrar exemplo

O exemplo a seguir mostra que os LIFs no clus2 reverteram para suas portas residenciais e mostra que os LIFs são revertidos com êxito se as portas na coluna porta atual tiverem um status de `true` na `Is Home` coluna. Se o `Is Home` valor for `false`, o LIF não foi revertido.

```
cluster::*> network interface show -role cluster
(network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

10. Verifique se as portas em cluster estão conetadas:

    `network port show`

Mostrar exemplo

O exemplo a seguir mostra o resultado do comando anterior `network port modify`, verificando se todas as interconexões de cluster são `up`:

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

11. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2        n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2        n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2        n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2        n1_clus2      none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. em cada nó no cluster, migre as interfaces associadas ao primeiro switch Nexus 5596, CL1, a ser substituído:

   ```
   network interface migrate
   ```

Mostrar exemplo

O exemplo a seguir mostra as portas ou LIFs que estão sendo migradas nos nós n1 e n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

2. Verifique o status do cluster:

   `network interface show`

Mostrar exemplo

O exemplo a seguir mostra que as LIFs de cluster necessárias foram migradas para portas de cluster apropriadas hospedadas no switch de cluster C2:

```
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0b     false
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0c     false
            n2_clus1   up/up      10.10.0.5/24       n2
e0b     false
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0c     false
8 entries were displayed.

----- ------- ----
```

3. Em todos os nós, encerre as portas dos nós que estão conectadas ao CL1:

   `network port modify`

Mostrar exemplo

O exemplo a seguir mostra as portas especificadas que estão sendo encerradas nos nós n1 e n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

4. Desligue as portas ISL 24, 31 e 32 no interrutor C2 ativo de 3132Q V:

   `shutdown`

   Mostrar exemplo

   O exemplo a seguir mostra como desligar ISLs 24, 31 e 32:

   ```
   C2# configure
   C2(Config)# interface e1/24/1-4
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# interface 1/31-32
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config-if)# exit
   C2#
   ```

5. Em todos os nós, remova todos os cabos conetados ao switch Nexus 5596 CL1.

   Com o cabeamento compatível, reconecte as portas desconetadas em todos os nós ao switch Nexus 3132Q-V C1.

6. Remova o cabo multicondutor QSFP das portas E1/24 do Nexus 3132Q-V C2.

   Conete as portas E1/31 e E1/32 no C1 às portas E1/31 e E1/32 no C2 usando fibra ótica Cisco QSFP ou cabos de conexão direta.

7. Restaure a configuração na porta 24 e remova o Canal de porta temporário 2 no C2:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

8. Abra as portas ISL 31 e 32 no C2, o interrutor ativo de 3132Q V: `no shutdown`

Mostrar exemplo

O exemplo a seguir mostra como abrir ISLs 31 e 32 no interrutor 3132Q-V C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

O que se segue?

"Conclua a migração".

Conclua a migração de switches Nexus 5596 para switches Nexus 3132Q-V.

Conclua as etapas a seguir para finalizar a migração de switches Nexus 5596 para switches Nexus 3132Q-V.

Passos

1. Verifique se as conexões ISL estão `up` no interrutor 3132Q-V C2:

```
show port-channel summary
```

Mostrar exemplo

As portas eth1/31 e eth1/32 devem indicar `(P)`, o que significa que ambas as portas ISL `up` estão no canal de porta:

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

2. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao novo switch de 3132Q V C1:

   `network port modify`

   Mostrar exemplo

   O exemplo a seguir mostra todas as portas de interconexão de cluster que estão sendo criadas para n1 e n2 no switch 3132Q-V C1:

   ```
   cluster::*> network port modify -node n1 -port e0a -up-admin true
   cluster::*> network port modify -node n1 -port e0d -up-admin true
   cluster::*> network port modify -node n2 -port e0a -up-admin true
   cluster::*> network port modify -node n2 -port e0d -up-admin true
   ```

3. Verifique o status da porta do nó do cluster:

   `network port show`

Mostrar exemplo

O exemplo a seguir verifica se todas as portas de interconexão de cluster em todos os nós no novo switch 3132Q-V C1 são `up`:

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

4. Em todos os nós, reverta as LIFs de cluster específicas para suas portas iniciais:

```
network interface revert
```

Mostrar exemplo

O exemplo a seguir mostra as LIFs de cluster específicas sendo revertidas para suas portas iniciais nos nós n1 e n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Verifique se a interface está em casa:

```
network interface show
```

Mostrar exemplo

O exemplo a seguir mostra o status das interfaces de interconexão de cluster é `up` e `Is home` para n1 e n2:

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
8 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------  -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2         n2_clus1       none
       3/5/2022 19:21:20 -06:00   n1_clus2         n2_clus2       none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2         n1_clus1       none
       3/5/2022 19:21:20 -06:00   n2_clus2         n1_clus2       none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

1. expanda o cluster adicionando nós aos switches de cluster Nexus 3132Q-V.
2. Exiba as informações sobre os dispositivos em sua configuração:
   - `network device-discovery show`

- network port show -role cluster
- network interface show -role cluster
- system cluster-switch show

Mostrar exemplo

Os exemplos a seguir mostram os nós n3 e n4 com portas de cluster de 40 GbE conetadas às portas E1/7 e E1/8, respetivamente nos switches de cluster Nexus 3132Q-V e ambos os nós aderiram ao cluster. As portas de interconexão de cluster de 40 GbE usadas são e4a e e4e.

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-
C3132Q-V
            e0b    C2                 Ethernet1/1/1    N3K-
C3132Q-V
            e0c    C2                 Ethernet1/1/2    N3K-
C3132Q-V
            e0d    C1                 Ethernet1/1/2    N3K-
C3132Q-V
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-
C3132Q-V
            e0b    C2                 Ethernet1/1/3    N3K-
C3132Q-V
            e0c    C2                 Ethernet1/1/4    N3K-
C3132Q-V
            e0d    C1                 Ethernet1/1/4    N3K-
C3132Q-V
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-
C3132Q-V
            e4e    C2                 Ethernet1/7      N3K-
C3132Q-V
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-
C3132Q-V
            e4e    C2                 Ethernet1/8      N3K-
C3132Q-V
12 entries were displayed.
```

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1
```

```
Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
```

```
-

Node: n4

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                           cluster-network   10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP

4 entries were displayed.
```

3. Remova o Nexus 5596 substituído se não forem removidos automaticamente:

   ```
   system cluster-switch delete
   ```

   Mostrar exemplo

   O exemplo a seguir mostra como remover o Nexus 5596:

   ```
   cluster::> system cluster-switch delete -device CL1
   cluster::> system cluster-switch delete -device CL2
   ```

4. Configure os clusters clus1 e clus2 para reverter automaticamente em cada nó e confirmar.

   Mostrar exemplo

   ```
   cluster::*> network interface modify -vserver node1 -lif clus1 -auto
   -revert true
   cluster::*> network interface modify -vserver node1 -lif clus2 -auto
   -revert true
   cluster::*> network interface modify -vserver node2 -lif clus1 -auto
   -revert true
   cluster::*> network interface modify -vserver node2 -lif clus2 -auto
   -revert true
   ```

5. Verifique se os switches de cluster adequados são monitorados:

   ```
   system cluster-switch show
   ```

Mostrar exemplo

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

6. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migre de clusters sem switch para clusters comutados de dois nós

Migre o fluxo de trabalho de clusters sem switch para clusters de dois nós

Siga estas etapas do fluxo de trabalho para migrar de um cluster sem switch de dois nós para um cluster comutado de dois nós que inclui os switches de rede de cluster Cisco Nexus 3132Q-V.

1 **"Requisitos de migração"**

Revise os requisitos e informações de exemplo do switch para o processo de migração.

2 **"Prepare-se para a migração"**

Prepare clusters sem switch para migração para clusters comutados de dois nós.

3 **"Configure as portas"**

Configure suas portas para migração de clusters sem switch de dois nós para clusters comutados de dois nós.

4 **"Conclua a migração"**

Conclua a migração de clusters sem switch para clusters com dois nós.

Requisitos de migração

Se você tiver um cluster sem switch de dois nós, revise este procedimento para os requisitos aplicáveis para migrar para um cluster comutado de dois nós.

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

Para obter mais informações, consulte:

- "NetApp CN1601 e CN1610"
- "Switch Ethernet Cisco"
- "Hardware Universe"

Conexões de porta e nó

Certifique-se de entender os requisitos de cabeamento e conexões de nó e porta ao migrar para um cluster comutado de dois nós com os switches de cluster Cisco Nexus 3132Q-V.

- Os switches do cluster usam as portas ISL (Inter-Switch Link) E1/31-32.
- O "Hardware Universe" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:
  - Os nós com conexões de cluster de 10 GbE exigem módulos óticos QSFP com cabos de fibra breakout ou cabos de rutura de cobre QSFP para SFP.
  - Os nós com conexões de cluster de 40 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.
  - Os switches de cluster usam o cabeamento ISL apropriado: Cabos de conexão direta de fibra 2x QSFP28 ou cobre.
- No Nexus 3132Q-V, você pode operar portas QSFP como modos Ethernet de 40 GB ou Ethernet 4x10 GB.

  Por padrão, existem 32 portas no modo Ethernet de 40 GB. Essas portas Ethernet de 40 GB são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta Ethernet de

40 GB é numerada como 1/2. O processo de alteração da configuração de Ethernet de 40 GB para Ethernet de 10 GB é chamado *breakout* e o processo de alteração da configuração de Ethernet de 10 GB para Ethernet de 40 GB é chamado *breakin*. Quando você divide uma porta Ethernet de 40 GB em portas Ethernet de 10 GB, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta Ethernet de 40 GB são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.

- No lado esquerdo do Nexus 3132Q-V está um conjunto de quatro portas SFP multiplexadas para a primeira porta QSFP.

  Por padrão, o RCF é estruturado para usar a primeira porta QSFP.

  Você pode ativar quatro portas SFP em vez de uma porta QSFP para Nexus 3132Q-V usando o `hardware profile front portmode sfp-plus` comando. Da mesma forma, você pode redefinir o Nexus 3132Q-V para usar uma porta QSFP em vez de quatro portas SFP usando o `hardware profile front portmode qsfp` comando.

- Certifique-se de que configurou algumas das portas no Nexus 3132Q-V para serem executadas a 10 GbE ou 40 GbE.

  Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP a partir da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- O número de portas de 10 GbE e 40 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Transferência do ficheiro de configuração de referência do comutador de rede de cluster da Cisco" .

Antes de começar

- Configurações corretamente configuradas e funcionando.
- Nós executando o ONTAP 9.4 ou posterior.
- Todas as portas de cluster `up` no estado.
- O switch de cluster Cisco Nexus 3132Q-V é suportado.
- A configuração de rede de cluster existente tem:
  - A infraestrutura de cluster do Nexus 3132 que é redundante e totalmente funcional em ambos os switches.
  - As versões mais recentes do RCF e NX-os em seus switches.

    "Switches Ethernet Cisco"tem informações sobre as versões do ONTAP e do NX-OS suportadas neste procedimento.

  - Conetividade de gerenciamento em ambos os switches.
  - Acesso ao console a ambos os switches.
  - Todas as interfaces lógicas de cluster (LIFs) no `up` estado sem serem migradas.
  - Personalização inicial do switch.
  - Todas as portas ISL ativadas e cabeadas.

Além disso, você precisa Planejar, migrar e ler a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.

Sobre os exemplos usados

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Switches de cluster Nexus 3132Q-V, C1 e C2.
- Os nós são n1 e n2.

> Os exemplos neste procedimento usam dois nós, cada um usando duas portas de interconexão de cluster de 40 GbE **e4a** e **e4e**. "Hardware Universe"O tem detalhes sobre as portas de cluster em suas plataformas.

Este procedimento abrange os seguintes cenários:

- **n1_clus1** é a primeira interface lógica de cluster (LIF) a ser conetada ao switch de cluster C1 para o nó **n1**.
- **n1_clus2** é o primeiro cluster LIF a ser conetado ao switch de cluster C2 para o nó **n1**.
- **n2_clus1** é o primeiro cluster LIF a ser conetado ao switch de cluster C1 para o nó **n2**.
- **n2_clus2** é o segundo LIF de cluster a ser conetado ao switch de cluster C2 para o nó **n2**.
- O número de portas de 10 GbE e 40 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Transferência do ficheiro de configuração de referência do comutador de rede de cluster da Cisco" .

> O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 3000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma.

- O cluster começa com dois nós conetados e funcionando em uma configuração de cluster sem switch de dois nós.
- A primeira porta de cluster é movida para C1.
- A segunda porta do cluster é movida para C2.
- A opção de cluster sem switch de dois nós está desativada.

O que se segue?

"Prepare-se para a migração".

Prepare-se para a migração de clusters sem switch para clusters comutados

Siga estas etapas para preparar seu cluster sem switch para migração para um cluster comutado de dois nós.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Determine o status administrativo ou operacional de cada interface de cluster:

   a. Exibir os atributos da porta de rede:

      `network port show`

      Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

   b. Exibir informações sobre as interfaces lógicas:

      `network interface show`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

3. Verifique se os RCFs e a imagem apropriados estão instalados nos novos switches 3132Q-V, conforme necessário, e faça qualquer personalização essencial do site, como usuários e senhas, endereços de rede, etc.

   Neste momento, tem de preparar ambos os interrutores. Se você precisar atualizar o RCF e o software de imagem, siga estas etapas:

   a. Vá para"Switches Ethernet Cisco" no site de suporte da NetApp .
   b. Observe o switch e as versões de software necessárias na tabela nessa página.
   c. Baixe a versão apropriada do RCF.
   d. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
   e. Transfira a versão apropriada do software de imagem.

4. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.

O que se segue?

"Configure as portas".

Configure suas portas para migração de clusters sem switch para clusters comutados

Siga estas etapas para configurar suas portas para migração de clusters sem switch de dois nós para clusters comutados de dois nós.

Passos

1. Nos switches Nexus 3132Q-V C1 e C2, desative todas as portas C1 e C2 voltadas para o nó, mas não desative as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 30 estão sendo desativadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração suportada no RCF : `NX3132_RCF_v1.1_24p10g_26p40g.txt`

```
C1# copy running-config startup-config
[########################################] 100%
Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit

C2# copy running-config startup-config
[########################################] 100%
Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

2. Conete as portas 1/31 e 1/32 no C1 às mesmas portas no C2 usando cabeamento compatível.
3. Verifique se as portas ISL estão operacionais no C1 e C2:

```
show port-channel summary
```

Mostrar exemplo

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)

C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

4. Exiba a lista de dispositivos vizinhos no switch:

   `show cdp neighbors`

Mostrar exemplo

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                 Eth1/31        174    R S I s     N3K-C3132Q-V
Eth1/31
C2                 Eth1/32        174    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                 Eth1/31        178    R S I s     N3K-C3132Q-V
Eth1/31
C1                 Eth1/32        178    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

5. Exiba a conetividade da porta do cluster em cada nó:

   `network device-discovery show`

Mostrar exemplo

O exemplo a seguir mostra uma configuração de cluster sem switch de dois nós.

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e4a    n2                   e4a              FAS9000
            e4e    n2                   e4e              FAS9000
n2         /cdp
            e4a    n1                   e4a              FAS9000
            e4e    n1                   e4e              FAS9000
```

6. Migre a interface clus1 para a porta física que hospeda o clus2:

   `network interface migrate`

   Execute este comando a partir de cada nó local.

   Mostrar exemplo

   ```
   cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
   -source-node n1
   -destination-node n1 -destination-port e4e
   cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
   -source-node n2
   -destination-node n2 -destination-port e4e
   ```

7. Verifique a migração das interfaces do cluster:

   `network interface show`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4e     false
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4e     false
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

8. Encerre as portas de cluster clus1 LIF em ambos os nós:

   `network port modify`

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

9. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2        n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2        n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2        n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2        n1_clus2      none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e4a 10.10.0.1
Cluster n1_clus2 n1     e4e 10.10.0.2
Cluster n2_clus1 n2     e4a 10.10.0.3
Cluster n2_clus2 n2     e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. Desconete o cabo do e4a no nó n1.

   Você pode consultar a configuração em execução e conetar a primeira porta de 40 GbE no switch C1 (porta 1/7 neste exemplo) a e4a no n1 usando cabeamento suportado no Nexus 3132Q-V.

   > Ao reconetar quaisquer cabos a um novo switch de cluster Cisco, os cabos usados devem ser de fibra ou cabeamento compatíveis com o Cisco.

2. Desconete o cabo do e4a no nó n2.

   Você pode consultar a configuração em execução e conetar o e4a à próxima porta de 40 GbE disponível no C1, porta 1/8, usando o cabeamento suportado.

3. Habilite todas as portas voltadas para nós no C1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 30 estão sendo habilitadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando a configuração suportada no RCF : `NX3132_RCF_v1.1_24p10g_26p40g.txt`

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

4. Ative a primeira porta de cluster, e4a, em cada nó:

   `network port modify`

   Mostrar exemplo

   ```
   cluster::*> network port modify -node n1 -port e4a -up-admin true
   cluster::*> network port modify -node n2 -port e4a -up-admin true
   ```

5. Verifique se os clusters estão ativos em ambos os nós:

   `network port show`

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

6. Para cada nó, reverta todas as LIFs de interconexão de cluster migradas:

   `network interface revert`

Mostrar exemplo

O exemplo a seguir mostra os LIFs migrados sendo revertidos para suas portas residenciais.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

7. Verifique se todas as portas de interconexão de cluster estão agora revertidas para suas portas iniciais:

   `network interface show`

   A `Is Home` coluna deve exibir um valor de `true` para todas as portas listadas na `Current Port` coluna. Se o valor exibido for `false`, a porta não foi revertida.

   Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

8. Exiba a conetividade da porta do cluster em cada nó:

   `network device-discovery show`

Mostrar exemplo

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3132Q-V
            e4e    n2                 e4e              FAS9000
n2         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3132Q-V
            e4e    n1                 e4e              FAS9000
```

9. No console de cada nó, migre clus2 para a porta e4a:

   `network interface migrate`

   Mostrar exemplo

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e4a
```

10. Encerre as portas de cluster clus2 LIF em ambos os nós:

    `network port modify`

    O exemplo a seguir mostra as portas especificadas sendo fechadas em ambos os nós:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

11. Verifique o status de LIF do cluster:

    `network interface show`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4a     false
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4a     false
4 entries were displayed.
```

12. Desconete o cabo do e4e no nó n1.

    Você pode consultar a configuração em execução e conetar a primeira porta de 40 GbE no switch C2 (porta 1/7 neste exemplo) a e4e no n1 usando cabeamento suportado no Nexus 3132Q-V.

13. Desconete o cabo do e4e no nó n2.

    Você pode consultar a configuração em execução e conetar o e4e à próxima porta de 40 GbE disponível no C2, porta 1/8, usando o cabeamento suportado.

14. Habilite todas as portas voltadas para nós no C2.

    Mostrar exemplo

    O exemplo a seguir mostra que as portas 1 a 30 estão sendo habilitadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração suportada no RCF : `NX3132_RCF_v1.1_24p10g_26p40g.txt`

    ```
    C2# configure
    C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
    4,e1/7-30
    C2(config-if-range)# no shutdown
    C2(config-if-range)# exit
    C2(config)# exit
    ```

15. Ative a segunda porta do cluster, e4e, em cada nó:

    `network port modify`

    O exemplo a seguir mostra as portas especificadas sendo criadas:

    ```
    cluster::*> network port modify -node n1 -port e4e -up-admin true
    cluster::*> network port modify -node n2 -port e4e -up-admin true
    ```

16. Para cada nó, reverta todas as LIFs de interconexão de cluster migradas:

    `network interface revert`

    O exemplo a seguir mostra os LIFs migrados sendo revertidos para suas portas residenciais.

    ```
    cluster::*> network interface revert -vserver Cluster -lif n1_clus2
    cluster::*> network interface revert -vserver Cluster -lif n2_clus2
    ```

17. Verifique se todas as portas de interconexão de cluster estão agora revertidas para suas portas iniciais:

    `network interface show`

    A `Is Home` coluna deve exibir um valor de `true` para todas as portas listadas na `Current Port` coluna. Se o valor exibido for `false`, a porta não foi revertida.

Mostrar exemplo

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

18. Verifique se todas as portas de interconexão de cluster estão no `up` estado.

    `network port show -role cluster`

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

O que se segue?

"Conclua a migração".

Concluir a migração de clusters sem switch de dois nós para clusters comutados de dois nós

Siga estas etapas para concluir a migração de clusters sem switch para clusters comutados de dois nós.

Passos

1. Exibir os números da porta do switch de cluster a que cada porta do cluster está conetada em cada nó:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
    cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e4a    C1                  Ethernet1/7      N3K-C3132Q-V
            e4e    C2                  Ethernet1/7      N3K-C3132Q-V
n2         /cdp
            e4a    C1                  Ethernet1/8      N3K-C3132Q-V
            e4e    C2                  Ethernet1/8      N3K-C3132Q-V
```

2. Exibir switches do cluster descobertos e monitorados:

   `system cluster-switch show`

Mostrar exemplo

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network      10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

3. Desative as configurações sem switch de dois nós em qualquer nó:

   `network options switchless-cluster`

```
network options switchless-cluster modify -enabled false
```

4. Verifique se a `switchless-cluster` opção foi desativada.

```
network options switchless-cluster show
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2        n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2        n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2        n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2        n1_clus2      none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e4a 10.10.0.1
Cluster n1_clus2 n1     e4e 10.10.0.2
Cluster n2_clus1 n2     e4a 10.10.0.3
Cluster n2_clus2 n2     e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os interrutores

Requisitos para a substituição de switches de cluster Cisco Nexus 3132Q-V.

Certifique-se de entender os requisitos de configuração, conexões de portas e requisitos de cabeamento ao substituir os switches de cluster.

Cisco Nexus 3132Q-V requisitos

- O switch de cluster Cisco Nexus 3132Q-V é suportado.
- O número de portas de 10 GbE e 40 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .

- Os switches do cluster usam as portas ISL (Inter-Switch Link) E1/31-32.
- O "Hardware Universe" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:
  - Os nós com conexões de cluster de 10 GbE exigem módulos óticos QSFP com cabos de fibra breakout ou cabos de rutura de cobre QSFP para SFP.
  - Os nós com conexões de cluster de 40 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.
  - Os switches de cluster usam o cabeamento ISL apropriado: Cabos de conexão direta de fibra 2x QSFP28 ou cobre.
- No Nexus 3132Q-V, você pode operar portas QSFP como modos Ethernet de 40 GB ou Ethernet 4x10 GB.

  Por padrão, existem 32 portas no modo Ethernet de 40 GB. Essas portas Ethernet de 40 GB são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta Ethernet de 40 GB é numerada como 1/2. O processo de alteração da configuração de Ethernet de 40 GB para Ethernet de 10 GB é chamado *breakout* e o processo de alteração da configuração de Ethernet de 10 GB para Ethernet de 40 GB é chamado *breakin*. Quando você divide uma porta Ethernet de 40 GB em portas Ethernet de 10 GB, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta Ethernet de 40 GB são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.

- No lado esquerdo do Nexus 3132Q-V está um conjunto de quatro portas SFP multiplexadas para a primeira porta QSFP.

  Por padrão, o RCF é estruturado para usar a primeira porta QSFP.

  Você pode ativar quatro portas SFP em vez de uma porta QSFP para Nexus 3132Q-V usando o `hardware profile front portmode sfp-plus` comando. Da mesma forma, você pode redefinir o Nexus 3132Q-V para usar uma porta QSFP em vez de quatro portas SFP usando o `hardware profile front portmode qsfp` comando.

- Você precisa ter configurado algumas das portas no Nexus 3132Q-V para ser executado a 10 GbE ou 40 GbE.

  Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP a partir da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você precisa ter feito o Planejamento, a migração e ler a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.

  "Switches Ethernet Cisco"tem informações sobre as versões do ONTAP e do NX-OS suportadas neste procedimento.

Cisco Nexus 5596 requisitos

- Os seguintes switches de cluster são suportados:
  - Nexus 5596
  - Nexus 3132Q-V
- O número de portas de 10 GbE e 40 GbE é definido nos arquivos de configuração de referência (RCFs)

disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .

- Os switches de cluster usam as seguintes portas para conexões com nós:
  - Portas E1/1-40 (10 GbE): Nexus 5596
  - Portas E1/1-30 (40 GbE): Nexus 3132Q-V
- Os switches do cluster usam as seguintes portas ISL (Inter-Switch Link):
  - Portas E1/41-48 (10 GbE): Nexus 5596
  - Portas E1/31-32 (40 GbE): Nexus 3132Q-V
- O "Hardware Universe" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:
  - Os nós com conexões de cluster de 10 GbE exigem cabos de conexões de fibra ótica QSFP para SFP ou cabos de conexões de cobre QSFP para SFP.
  - Os nós com conexões de cluster de 40 GbE exigem módulos QSFP/QSFP28optical com cabos de fibra ou cabos de conexão direta de cobre QSFP/QSFP28.
- Os switches de cluster usam o cabeamento ISL apropriado:
  - Início: Nexus 5596X para Nexus 5596X (SFP para SFP)
    - 8x cabos de conexão direta de fibra ou cobre SFP
  - Interino: Nexus 5596 para Nexus 3132Q-V (QSFP para mais de 4xSFP break-out)
    - 1x cabos de rutura de fibra QSFP para SFP ou de rutura de cobre
  - Final: Nexus 3132Q-V para Nexus 3132Q-V (QSFP28 a QSFP28)
    - 2x QSFP28 cabos de ligação direta de fibra ou cobre
- Nos switches Nexus 3132Q-V, você pode operar portas QSFP/QSFP28 como modos 40 Gigabit Ethernet ou 4 x10 Gigabit Ethernet.

  Por padrão, existem 32 portas no modo 40 Gigabit Ethernet. Essas 40 portas Gigabit Ethernet são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta 40 Gigabit Ethernet é numerada como 1/2. O processo de alteração da configuração de 40 Gigabit Ethernet para 10 Gigabit Ethernet é chamado *breakout* e o processo de alteração da configuração de 10 Gigabit Ethernet para 40 Gigabit Ethernet é chamado *breakin*. Quando você divide uma porta Ethernet de 40 Gigabit em 10 portas Gigabit Ethernet, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta 40 Gigabit Ethernet são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.

- No lado esquerdo dos switches Nexus 3132Q-V está um conjunto de 4 portas SFP multiplexadas para essa porta QSFP28.

  Por padrão, o RCF é estruturado para usar a porta QSFP28.

  > Você pode tornar 4x portas SFP mais ativas em vez de uma porta QSFP para switches Nexus 3132Q-V usando o `hardware profile front portmode sfp-plus` comando. Da mesma forma, você pode redefinir os switches Nexus 3132Q-V para usar uma porta QSFP em vez de 4x portas SFP usando o `hardware profile front portmode qsfp` comando.

- Você configurou algumas das portas nos switches Nexus 3132Q-V para serem executadas a 10 GbE ou 40 GbE.

Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP a partir da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você fez o Planejamento, a migração e leu a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.
- As versões ONTAP e NX-OS suportadas neste procedimento estão em"Switches Ethernet Cisco" .

Requisitos do NetApp CN1610

- Os seguintes switches de cluster são suportados:
  - NetApp CN1610
  - Cisco Nexus 3132Q-V
- Os switches do cluster suportam as seguintes conexões de nós:
  - NetApp CN1610: Portas de 0/1 a 0/12 (10 GbE)
  - Cisco Nexus 3132QP-V: Portas E1/1-30 (40 GbE)
- Os interrutores do grupo de instrumentos utilizam as seguintes portas ISL (Inter-Switch Link):
  - NetApp CN1610: Portas de 0/13 a 0/16 (10 GbE)
  - Cisco Nexus 3132QP-V: Portas E1/31-32 (40 GbE)
- O "Hardware Universe" contém informações sobre cabeamento compatível com switches Nexus 3132Q-V:
  - Os nós com conexões de cluster de 10 GbE exigem cabos de conexões de fibra ótica QSFP para SFP ou cabos de conexões de cobre QSFP para SFP
  - Os nós com conexões de cluster de 40 GbE exigem módulos óticos QSFP/QSFP28 com cabos de fibra ótica ou cabos de conexão direta de cobre QSFP/QSFP28
- O cabeamento ISL apropriado é o seguinte:
  - Início: Para CN1610 GbE a CN1610 GbE (SFP a SFP), quatro cabos de conexão direta de fibra ótica SFP ou cobre
  - Interino: Para CN1610 para Nexus 3132Q-V (QSFP para quatro SFP mais breakout), um cabo de fibra ótica QSFP para SFP ou de cobre breakout
  - Final: Para Nexus 3132Q-V para Nexus 3132Q-V (QSFP28 a QSFP28), dois cabos de fibra ótica QSFP28 ou cobre de ligação direta
- Os cabos NetApp twinax não são compatíveis com os switches Cisco Nexus 3132Q-V.

  Se a sua configuração atual do CN1610 utilizar cabos NetApp twinax para ligações de cluster-nó-a-switch ou ISL e pretender continuar a utilizar o twinax no seu ambiente, tem de adquirir cabos Cisco twinax. Como alternativa, você pode usar cabos de fibra ótica tanto para as conexões ISL quanto para as conexões cluster-node para switch.

- Nos switches Nexus 3132Q-V, você pode operar portas QSFP/QSFP28 como modos Ethernet de 40 GB ou Ethernet de 4x 10 GB.

  Por padrão, existem 32 portas no modo Ethernet de 40 GB. Essas portas Ethernet de 40 GB são numeradas em uma convenção de nomenclatura de 2 tuplos. Por exemplo, a segunda porta Ethernet de 40 GB é numerada como 1/2. O processo de alteração da configuração de Ethernet de 40 GB para Ethernet de 10 GB é chamado *breakout* e o processo de alteração da configuração de Ethernet de 10 GB

para Ethernet de 40 GB é chamado *breakin*. Quando você divide uma porta Ethernet de 40 GB em portas Ethernet de 10 GB, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 tuplas. Por exemplo, as portas de saída da segunda porta Ethernet de 40 GB são numeradas como 1/2/1, 1/2/2, 1/2/4 e 1/2/3.

- No lado esquerdo dos switches Nexus 3132Q-V está um conjunto de quatro portas SFP multiplexadas para a primeira porta QSFP.

  Por padrão, o arquivo de configuração de referência (RCF) é estruturado para usar a primeira porta QSFP.

  Você pode ativar quatro portas SFP em vez de uma porta QSFP para switches Nexus 3132Q-V usando o `hardware profile front portmode sfp-plus` comando. Da mesma forma, você pode redefinir os switches Nexus 3132Q-V para usar uma porta QSFP em vez de quatro portas SFP usando o `hardware profile front portmode qsfp` comando.

  > Quando você usa as primeiras quatro portas SFP, ele desativará a primeira porta QSFP de 40GbE GbE.

- Você deve ter configurado algumas das portas nos switches Nexus 3132Q-V para serem executados a 10 GbE ou 40 GbE.

  Você pode dividir as primeiras seis portas no modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as primeiras seis portas QSFP da configuração *breakout* usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você precisa ter feito o Planejamento, a migração e ler a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.
- As versões ONTAP e NX-OS suportadas neste procedimento estão listadas em"Switches Ethernet Cisco" .
- As versões ONTAP e FASTPATH suportadas neste procedimento estão listadas em"Switches NetApp CN1601 e CN1610" .

Substitua os switches do cluster Cisco Nexus 3132Q-V.

Siga este procedimento para substituir um switch Cisco Nexus 3132Q-V defeituoso em uma rede de cluster. O procedimento de substituição é um procedimento sem interrupções (NDO).

Rever os requisitos

Requisitos do interrutor

Reveja o "Requisitos para a substituição de switches de cluster Cisco Nexus 3132Q-V.".

Antes de começar

- O cluster e a configuração de rede existentes têm:
  - A infraestrutura de cluster Nexus 3132Q-V é redundante e totalmente funcional em ambos os switches.

    "Switch Ethernet Cisco"tem as versões mais recentes de RCF e NX-OS para seus switches.

  - Todas as portas do cluster estão `up` no estado.

- A conetividade de gerenciamento existe em ambos os switches.
- Todas as interfaces lógicas de cluster (LIFs) estão no `up` estado e foram migradas.

- Para o interrutor de substituição Nexus 3132Q-V, certifique-se de que:
  - A conetividade de rede de gerenciamento no switch de substituição está funcional.
  - O acesso do console ao interrutor de substituição está no lugar.
  - O interrutor de imagem do sistema operativo RCF e NX-os pretendido é carregado no interrutor.
  - A personalização inicial do switch está concluída.
- "Hardware Universe"

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desabilitar a criação de casos durante a manutenção. Veja este artigo da Base de Conhecimento"SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para mais detalhes.
- Habilite o registro de sessão para qualquer sessão CLI. Para obter instruções sobre como habilitar o registro de sessão, revise a seção "Registro de saída de sessão" neste artigo da Base de conhecimento"Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Substitua o interrutor

Este procedimento substitui o segundo interrutor de cluster Nexus 3132Q C2-V CL2 com o novo interrutor de 3132Q-V.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- N1_clus1 é a primeira interface lógica de cluster (LIF) conetada ao switch de cluster C1 para o nó n1.
- N1_clus2 é o primeiro cluster LIF conetado ao switch de cluster CL2 ou C2, para o nó n1.
- N1_clus3 é o segundo LIF conetado ao switch de cluster C2, para o nó n1.
- N1_clus4 é o segundo LIF conetado ao switch de cluster CL1, para o nó n1.
- O número de portas de 10 GbE e 40 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis em"Download do arquivo de configuração de referência do comutador de rede de cluster Cisco" .
- Os nós são n1, n2, n3 e n4. - Os exemplos neste procedimento usam quatro nós: Dois nós usam quatro portas de interconexão de cluster de 10 GB: e0a, e0b, e0c e e0d. Os outros dois nós usam duas portas de interconexão de cluster de 40 GB: e4a e e4e. Consulte a "Hardware Universe" para ver as portas de cluster reais nas suas plataformas.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O cluster começa com quatro nós conectados a dois switches de cluster Nexus 3132Q-V, CL1 e CL2.
- O interrutor do cluster CL2 deve ser substituído pelo C2

- Em cada nó, as LIFs de cluster conetadas ao CL2 são migradas para portas de cluster conetadas ao CL1.
- Desconete o cabeamento de todas as portas do CL2 e reconete o cabeamento às mesmas portas do switch de substituição C2.
- Em cada nó, suas LIFs de cluster migradas são revertidas.

Passo 1: Prepare-se para a substituição

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Exiba informações sobre os dispositivos em sua configuração:

   ```
   network device-discovery show
   ```

Mostrar exemplo

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface         Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    CL1                Ethernet1/1/1    N3K-C3132Q-V
            e0b    CL2                Ethernet1/1/1    N3K-C3132Q-V
            e0c    CL2                Ethernet1/1/2    N3K-C3132Q-V
            e0d    CL1                Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    CL1                Ethernet1/1/3    N3K-C3132Q-V
            e0b    CL2                Ethernet1/1/3    N3K-C3132Q-V
            e0c    CL2                Ethernet1/1/4    N3K-C3132Q-V
            e0d    CL1                Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    CL1                Ethernet1/7      N3K-C3132Q-V
            e4e    CL2                Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    CL1                Ethernet1/8      N3K-C3132Q-V
            e4e    CL2                Ethernet1/8      N3K-C3132Q-V

12 entries were displayed
```

3. Determine o status administrativo ou operacional de cada interface de cluster:

   a. Exibir os atributos da porta de rede:

      ```
      network port show
      ```

Mostrar exemplo

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                      Speed(Mbps)
Health   Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                   Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas:

```
network interface show
```

Mostrar exemplo

```
cluster::*> network interface show -role cluster
       (network interface show)

             Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true

12 entries were displayed.
```

c. Exiba as informações nos switches do cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                          cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

4. Verifique se o RCF e a imagem apropriados estão instalados no novo switch Nexus 3132Q-V, conforme necessário, e faça qualquer personalização essencial do site.

   Neste momento, tem de preparar o interrutor de substituição. Se você precisar atualizar o RCF e a imagem, siga estas etapas:

   a. No site de suporte da NetApp , consulte"Switches Ethernet Cisco" .
   b. Observe o switch e as versões de software necessárias na tabela nessa página.
   c. Baixe a versão apropriada do RCF.
   d. Clique em **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.
   e. Transfira a versão apropriada do software de imagem.

5. Migre os LIFs associados às portas de cluster conetadas ao switch C2:

   `network interface migrate`

Mostrar exemplo

Este exemplo mostra que a migração de LIF é feita em todos os nós:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 –destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 –destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 –destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 –destination-node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 –destination-node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 –destination-node n4 -destination-port e4a
```

6. Verifique a integridade do cluster:

   `network interface show`

Mostrar exemplo

```
cluster::*> network interface show -role cluster
       (network interface show)

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0a     false
            n1_clus3   up/up      10.10.0.3/24       n1
e0d     false
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0a     false
            n2_clus3   up/up      10.10.0.7/24       n2
e0d     false
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4a     false
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4a     false
12 entries were displayed.
```

7. Encerre as portas de interconexão de cluster que estão fisicamente conetadas ao switch CL2:

   `network port modify`

Mostrar exemplo

Este exemplo mostra as portas especificadas que estão sendo encerradas em todos os nós:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source     Destination   Packet
Node   Date                       LIF        LIF           Loss
------ -------------------------- ---------- ------------- -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2      none
n3
...
...
n4
...
...
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

`cluster ping-cluster -node <name>`

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
```

```
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8
Cluster n3_clus1 n4     e0a 10.10.0.9
Cluster n3_clus2 n3     e0e 10.10.0.10
Cluster n4_clus1 n4     e0a 10.10.0.11
Cluster n4_clus2 n4     e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
```

```
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

1. desligue as portas 1/31 e 1/32 no CL1 e o switch Nexus 3132Q-V ativo:

   `shutdown`

   Mostrar exemplo

   Este exemplo mostra as portas ISL 1/31 e 1/32 sendo fechadas no interrutor CL1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/31-32
   (CL1)(config-if-range)# shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

Etapa 2: Configurar portas

1. Remova todos os cabos conetados ao switch Nexus 3132Q-V CL2 e reconete-os ao switch de substituição C2 em todos os nós.
2. Retire os cabos ISL das portas E1/31 e E1/32 no CL2 e volte a ligá-los às mesmas portas no interrutor de substituição C2.
3. Abra as portas ISLs 1/31 e 1/32 no switch Nexus 3132Q-V CL1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/31-32
   (CL1)(config-if-range)# no shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

4. Verifique se os ISLs estão acima em CL1:

   `show port-channel`

As portas eth1/31 e eth1/32 devem indicar `(P)`, o que significa que as portas ISL estão no canal da porta.

Mostrar exemplo

```
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member
Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

5. Verifique se os ISLs estão acima em C2:

`show port-channel summary`

As portas eth1/31 e eth1/32 devem indicar `(P)`, o que significa que ambas as portas ISL estão no canal de porta.

Mostrar exemplo

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

6. Em todos os nós, abra todas as portas de interconexão de cluster conetadas ao switch Nexus 3132Q-V C2:

   `network port modify`

   Mostrar exemplo

   ```
   cluster::*> network port modify -node n1 -port e0b -up-admin true
   cluster::*> network port modify -node n1 -port e0c -up-admin true
   cluster::*> network port modify -node n2 -port e0b -up-admin true
   cluster::*> network port modify -node n2 -port e0c -up-admin true
   cluster::*> network port modify -node n3 -port e4e -up-admin true
   cluster::*> network port modify -node n4 -port e4e -up-admin true
   ```

7. Para todos os nós, reverta todas as LIFs de interconexão de cluster migradas:

   `network interface revert`

   Mostrar exemplo

   ```
   cluster::*> network interface revert -vserver Cluster -lif n1_clus2
   cluster::*> network interface revert -vserver Cluster -lif n1_clus3
   cluster::*> network interface revert -vserver Cluster -lif n2_clus2
   cluster::*> network interface revert -vserver Cluster -lif n2_clus3
   cluster::*> network interface revert -vserver Cluster -lif n3_clus2
   cluster::*> network interface revert -vserver Cluster -lif n4_clus2
   ```

8. Verifique se as portas de interconexão de cluster estão agora revertidas para sua casa:

   `network interface show`

Mostrar exemplo

Este exemplo mostra que todos os LIFs são revertidos com sucesso porque as portas listadas na `Current Port` coluna têm um status de `true` na `Is Home` coluna. Se o `Is Home` valor da coluna for `false`, o LIF não foi revertido.

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

9. Verifique se as portas do cluster estão conetadas:

   `network port show`

Mostrar exemplo

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
```

```
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

10. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o comando show para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                Source     Destination   Packet
Node   Date                     LIF        LIF           Loss
------ ------------------------ ---------- ------------- -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2      none
n3
...
...
n4
...
...
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

`cluster ping-cluster -node <name>`

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8
```

```
Cluster n3_clus1 n3     e0a 10.10.0.9
Cluster n3_clus2 n3     e0e 10.10.0.10
Cluster n4_clus1 n4     e0a 10.10.0.11
Cluster n4_clus2 n4     e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
```

```
    Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Etapa 3: Verifique a configuração

1. Exiba as informações sobre os dispositivos em sua configuração:
    - `network device-discovery show`
    - `network port show -role cluster`
    - `network interface show -role cluster`
    - `system cluster-switch show`

Mostrar exemplo

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/1    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/2    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/3    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/4    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3132Q-V
            e4e    C2                 Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3132Q-V
            e4e    C2                 Ethernet1/8      N3K-C3132Q-V
12 entries were displayed.
```

```
cluster::*> network port show –role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-
```

```
Node: n2

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
```

```
12 entries were displayed.
```

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                          cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP
C2                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000003
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

3 entries were displayed.
```

2. Retire o interrutor Nexus 3132Q-V substituído, se ainda não for removido automaticamente:

   `system cluster-switch delete`

```
cluster::*> system cluster-switch delete –device CL2
```

3. Verifique se os switches de cluster adequados são monitorados:

   `system cluster-switch show`

   Mostrar exemplo

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network    10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.103
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

4. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=END`

O que se segue?

"Configurar o monitoramento de integridade do switch"

Substitua os switches de cluster Cisco Nexus 3132Q-V por conexões sem switch

No ONTAP 9.3 e versões posteriores, você pode migrar de um cluster com uma rede de cluster comutada para uma onde dois nós estão conectados diretamente.

A NetApp recomenda que você atualize sua versão do ONTAP antes de prosseguir com a operação de cluster comutado para sem switch para switches Cisco Nexus 3132Q-V.

Consulte o seguinte para obter mais detalhes:

- "SU540: Erros de NIC Chelsio T6 causam desligamento do sistema ao atualizar switches de rede de 40G para 100G"
- "Pânico de nó após migração de cluster comutado para cluster sem comutação"

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

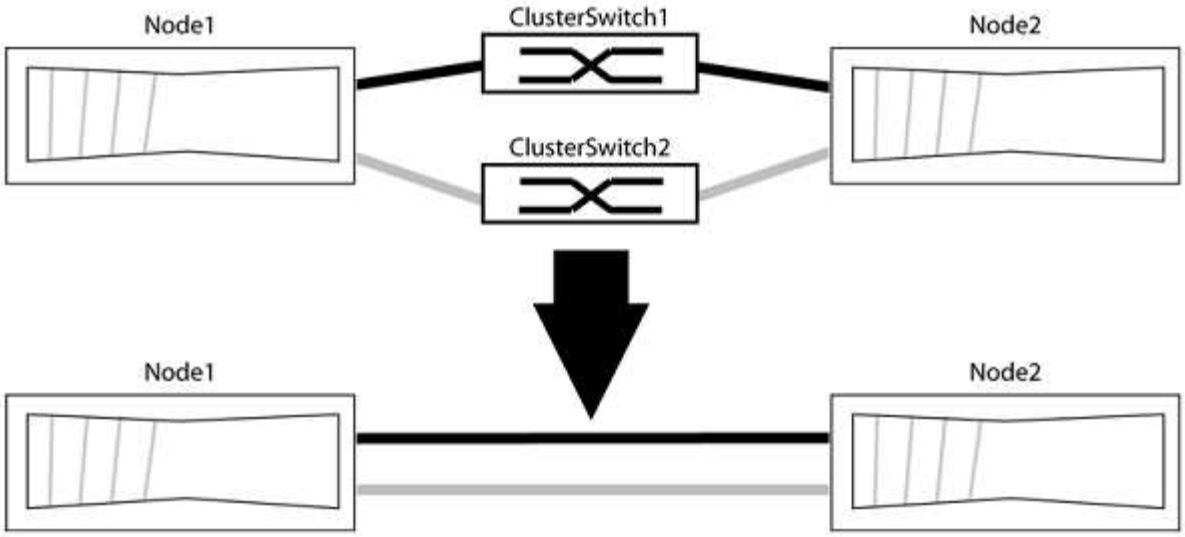
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

   ```
   network options detect-switchless-cluster show
   ```

   Mostrar exemplo

   A saída de exemplo a seguir mostra se a opção está ativada.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

`h`onde está a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico desta tarefa de manutenção para que possa suprimir a criação automática de casos durante a janela de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

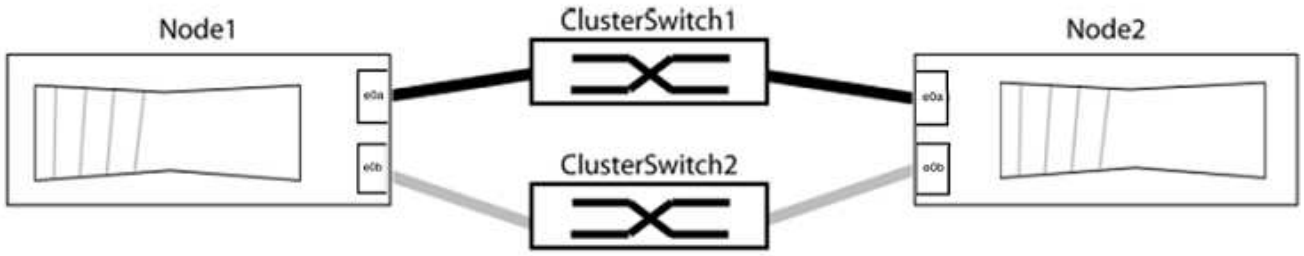
Mostrar exemplo

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-cisco-3132q-v/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



   Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

   Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

   `network interface show -vserver Cluster -fields is-home`

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

```
network interface revert -vserver Cluster -lif *
```

4. Desativar a reversão automática para as LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

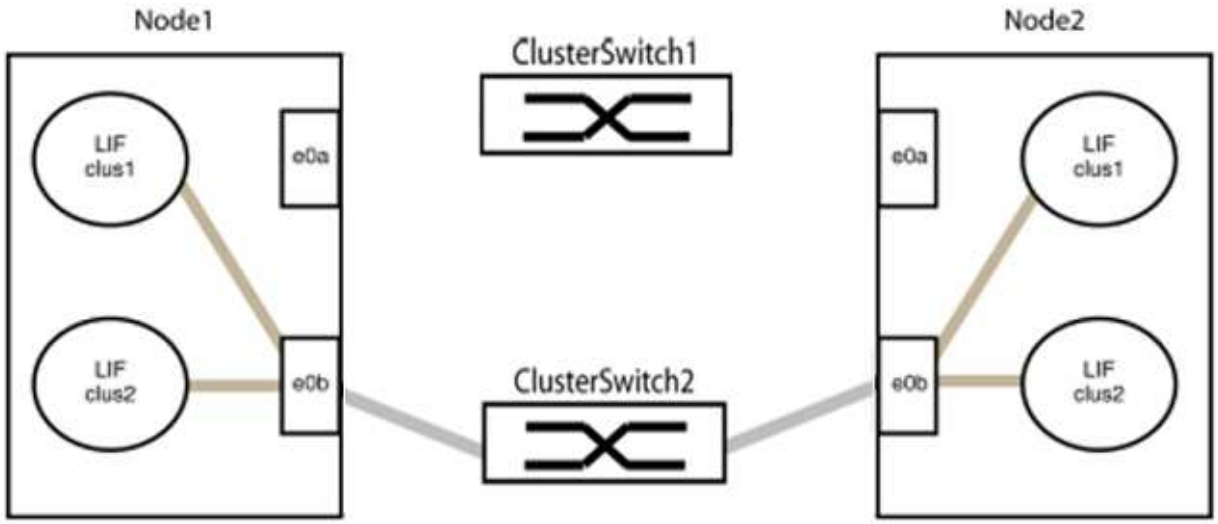
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

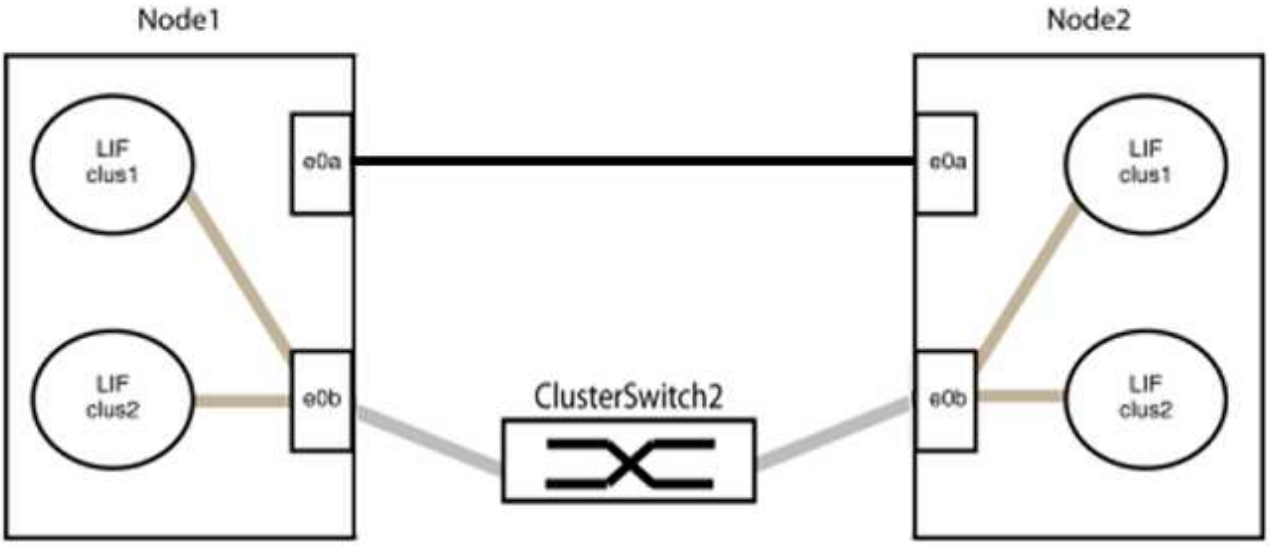
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

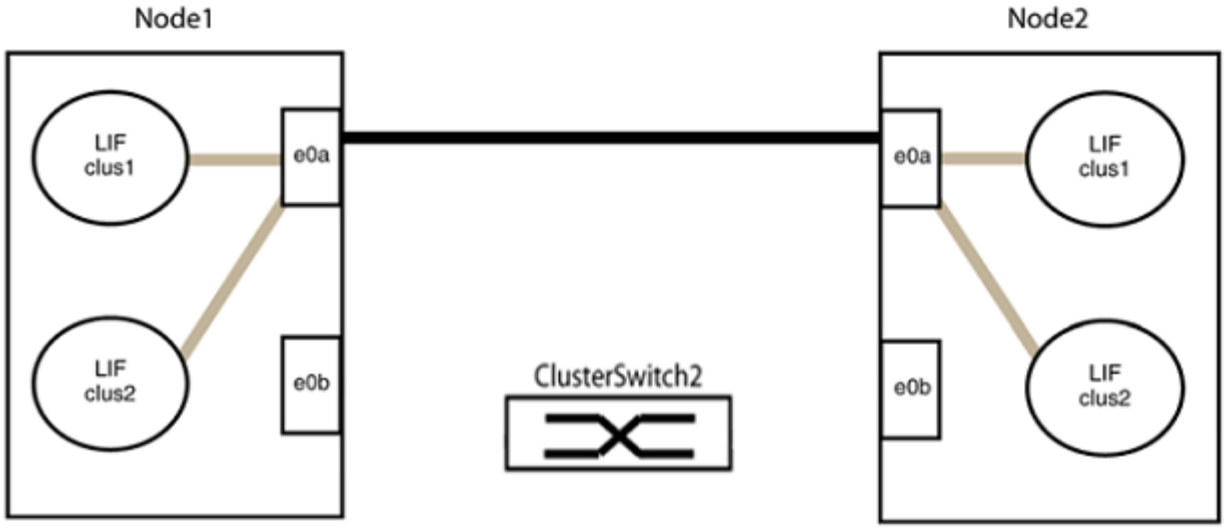
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

   No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

   `network device-discovery show -port cluster_port`

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

Cisco Nexus 92300YC

Comece agora

Fluxo de trabalho de instalação e configuração para switches Cisco Nexus 92300YC

Os switches Cisco Nexus 92300YC podem ser usados como switches de cluster no seu cluster AFF ou FAS . Os switches de cluster permitem que você crie clusters ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seu switch Cisco Nexus 92300YC.

1. **"Requisitos de configuração"**

Revise os requisitos de configuração para o switch de cluster 92300YC.

2. **"Documentação necessária"**

Revise a documentação específica do switch e do controlador para configurar seus switches 92300YC e o cluster ONTAP .

3. **"Requisitos para Smart Call Home"**

Revise os requisitos do recurso Cisco Smart Call Home, usado para monitorar os componentes de hardware e software na sua rede.

4. **"Instale o hardware"**

Instale o hardware do switch.

5. **"Configurar o software"**

Configure o software do switch.

Requisitos de configuração para switches Cisco Nexus 92300YC

Para instalação e manutenção do switch Cisco Nexus 92300YC, certifique-se de rever todos os requisitos de configuração e rede.

Se você quiser criar clusters do ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar switches de gerenciamento adicionais, que são opcionais.

Requisitos de configuração

Para configurar o cluster, é necessário o número e o tipo apropriados de cabos e conetores de cabos para os switches. Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conetar à porta do console do switch com o cabo de console incluído; você também precisa fornecer informações específicas de rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para o tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de storage e todos os switches aplicáveis
- A maioria dos controladores do sistema de storage é gerenciada por meio da interface e0M, conetando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700, a interface e0M utiliza uma porta Ethernet dedicada.

Consulte a "Hardware Universe" para obter informações mais recentes.

O que vem a seguir

"Componentes e números de peça" .

Componentes e números de peça para switches Cisco Nexus 92300YC

Para a instalação e manutenção do switch Cisco Nexus 92300YC, certifique-se de rever todos os componentes e números de peça do switch. Consulte "Hardware Universe" para obter detalhes.

A tabela a seguir lista o número de peça e a descrição do interrutor 92300YC, ventiladores e fontes de alimentação:

Número de peça	Descrição
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN
X-NXA-FAN-35CFM-B	Ventilador, fluxo de ar de admissão lateral da porta Cisco N9K
X-NXA-FAN-35CFM-F	Ventilador, fluxo de ar de escape lateral da porta Cisco N9K
X-NXA-PAC-650W-B	Fonte de alimentação, Cisco 650W - Entrada lateral da porta
X-NXA-PAC-650W-F	Fonte de alimentação, Cisco 650W - escape lateral da porta

Detalhes do fluxo de ar do switch Cisco Nexus 92300YC:

- Fluxo de ar do escape do lado do pórtico (ar padrão) — o ar frio entra no chassi através dos módulos do ventilador e da fonte de alimentação no corredor frio e esgota através da extremidade do pórtico do chassi no corredor quente. Fluxo de ar do escape do lado da porta com coloração azul.
- Fluxo de ar de entrada do lado do pórtico (ar reverso) — o ar frio entra no chassi através da extremidade do pórtico no corredor frio e esgota através dos módulos do ventilador e da fonte de alimentação no corredor quente. Fluxo de ar de admissão do lado do porto com coloração Borgonha.

O que vem a seguir

"Documentação necessária" .

Requisitos de documentação para switches Cisco Nexus 92300YC

Para instalação e manutenção do switch Cisco Nexus 92300YC, certifique-se de rever toda a documentação recomendada.

Documentação do switch

Para configurar os switches Cisco Nexus 92300YC, você precisa da seguinte documentação do "Suporte para switches Cisco Nexus 9000 Series" página:

Título do documento	Descrição
Guia de Instalação de hardware da Série Nexus 9000	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
Guias de configuração do software de comutador da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações de configuração inicial do switch que você precisa antes de configurar o switch para operação ONTAP.
Guia de atualização e downgrade do software NX-os da série Cisco Nexus 9000 (escolha o guia para a versão NX-os instalada em seus switches)	Fornece informações sobre como fazer downgrade do switch para o software de switch suportado pelo ONTAP, se necessário.
Cisco Nexus 9000 Series NX-os Guia de Referência de comando	Fornece links para as várias referências de comando fornecidas pelo Cisco.
Cisco Nexus 9000 MIBs Referência	Descreve os arquivos MIB (Management Information base) para os switches Nexus 9000.
Nexus 9000 Series NX-os System Message Reference	Descreve as mensagens do sistema para os switches da série Cisco Nexus 9000, aqueles que são informativos e outros que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de lançamento do Cisco Nexus 9000 Series NX-os (escolha as notas para a versão NX-os instalada em seus switches)	Descreve os recursos, bugs e limitações do Cisco Nexus 9000 Series.
Conformidade regulamentar e informações de segurança para a série Cisco Nexus 9000	Fornece informações legais, de conformidade, segurança e conformidade de agências internacionais para os switches da série Nexus 9000.

Documentação de sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para sua versão do sistema operacional "ONTAP 9" .

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar hardware NetApp.

Nome	Descrição
Documentação do ONTAP	Fornece informações detalhadas sobre todos os aspetos das versões do ONTAP.
"Hardware Universe"	Fornece informações de compatibilidade e configuração de hardware NetApp.

Kit de trilho e documentação do gabinete

Para instalar um switch Cisco Nexus 92300YC em um gabinete NetApp, consulte a documentação de hardware a seguir.

Nome	Descrição
"Armário do sistema 42U, guia profundo"	Descreve as FRUs associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição da FRU.
"Instalar um switch Cisco Nexus 92300YC em um gabinete NetApp"	Descreve como instalar um switch Cisco Nexus 92300YC em um gabinete NetApp de quatro colunas.

Requisitos para Smart Call Home

Para usar o Smart Call Home, você deve configurar um switch de rede de cluster para se comunicar por e-mail com o sistema Smart Call Home. Além disso, você pode opcionalmente configurar seu switch de rede de cluster para aproveitar o recurso de suporte Smart Call Home incorporado da Cisco.

O Smart Call Home monitora os componentes de hardware e software na sua rede. Quando ocorre uma configuração crítica do sistema, ele gera uma notificação por e-mail e envia um alerta para todos os destinatários configurados no seu perfil de destino.

Antes de usar o Smart Call Home, esteja ciente dos seguintes requisitos:

- Um servidor de e-mail deve estar no lugar.
- O switch deve ter conetividade IP com o servidor de e-mail.
- É necessário configurar o nome do contacto (contacto do servidor SNMP), o número de telefone e as informações do endereço da rua. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID de CCO deve ser associado a um contrato de serviço Cisco SMARTnet apropriado para a sua empresa.
- O Serviço SMARTnet da Cisco deve estar em vigor para que o dispositivo seja registrado.

O "Site de suporte da Cisco" contém informações sobre os comandos para configurar Smart Call Home.

Instale o hardware

Fluxo de trabalho de instalação de hardware para switches Cisco Nexus 92300YC

Para instalar e configurar o hardware de um switch de cluster 92300YC, siga estas etapas:

1. **"Preencha a planilha de cabeamento"**

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

2. **"Instale o interrutor"**

Instale o switch 92300YC.

3. **"Instale o interrutor em um gabinete NetApp"**

Instale o switch 92300YC e o painel de passagem em um gabinete NetApp , conforme necessário.

4. **"Revise o cabeamento e a configuração"**

Revise o suporte para portas Ethernet NVIDIA .

Folha de cálculo completa de cabeamento do Cisco Nexus 92300YC

Se você quiser documentar as plataformas suportadas, baixe um PDF desta página e complete a Planilha de cabeamento.

A Planilha de exemplo de cabeamento fornece exemplos de atribuições de portas recomendadas dos switches para os controladores. A Planilha em branco fornece um modelo que você pode usar na configuração do cluster.

Planilha de cabeamento de amostra

A definição de porta de amostra em cada par de switches é a seguinte:

Interrutor do cluster A		**Interrutor B do grupo de instrumentos**	
Porta do switch	Uso de nó e porta	Porta do switch	Uso de nó e porta
1	Nó de 10/25 GbE	1	Nó de 10/25 GbE
2	Nó de 10/25 GbE	2	Nó de 10/25 GbE
3	Nó de 10/25 GbE	3	Nó de 10/25 GbE
4	Nó de 10/25 GbE	4	Nó de 10/25 GbE

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
5	Nó de 10/25 GbE	5	Nó de 10/25 GbE
6	Nó de 10/25 GbE	6	Nó de 10/25 GbE
7	Nó de 10/25 GbE	7	Nó de 10/25 GbE
8	Nó de 10/25 GbE	8	Nó de 10/25 GbE
9	Nó de 10/25 GbE	9	Nó de 10/25 GbE
10	Nó de 10/25 GbE	10	Nó de 10/25 GbE
11	Nó de 10/25 GbE	11	Nó de 10/25 GbE
12	Nó de 10/25 GbE	12	Nó de 10/25 GbE
13	Nó de 10/25 GbE	13	Nó de 10/25 GbE
14	Nó de 10/25 GbE	14	Nó de 10/25 GbE
15	Nó de 10/25 GbE	15	Nó de 10/25 GbE
16	Nó de 10/25 GbE	16	Nó de 10/25 GbE
17	Nó de 10/25 GbE	17	Nó de 10/25 GbE
18	Nó de 10/25 GbE	18	Nó de 10/25 GbE
19	Nó de 10/25 GbE	19	Nó de 10/25 GbE
20	Nó de 10/25 GbE	20	Nó de 10/25 GbE
21	Nó de 10/25 GbE	21	Nó de 10/25 GbE
22	Nó de 10/25 GbE	22	Nó de 10/25 GbE
23	Nó de 10/25 GbE	23	Nó de 10/25 GbE
24	Nó de 10/25 GbE	24	Nó de 10/25 GbE
25	Nó de 10/25 GbE	25	Nó de 10/25 GbE
26	Nó de 10/25 GbE	26	Nó de 10/25 GbE

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
27	Nó de 10/25 GbE	27	Nó de 10/25 GbE
28	Nó de 10/25 GbE	28	Nó de 10/25 GbE
29	Nó de 10/25 GbE	29	Nó de 10/25 GbE
30	Nó de 10/25 GbE	30	Nó de 10/25 GbE
31	Nó de 10/25 GbE	31	Nó de 10/25 GbE
32	Nó de 10/25 GbE	32	Nó de 10/25 GbE
33	Nó de 10/25 GbE	33	Nó de 10/25 GbE
34	Nó de 10/25 GbE	34	Nó de 10/25 GbE
35	Nó de 10/25 GbE	35	Nó de 10/25 GbE
36	Nó de 10/25 GbE	36	Nó de 10/25 GbE
37	Nó de 10/25 GbE	37	Nó de 10/25 GbE
38	Nó de 10/25 GbE	38	Nó de 10/25 GbE
39	Nó de 10/25 GbE	39	Nó de 10/25 GbE
40	Nó de 10/25 GbE	40	Nó de 10/25 GbE
41	Nó de 10/25 GbE	41	Nó de 10/25 GbE
42	Nó de 10/25 GbE	42	Nó de 10/25 GbE
43	Nó de 10/25 GbE	43	Nó de 10/25 GbE
44	Nó de 10/25 GbE	44	Nó de 10/25 GbE
45	Nó de 10/25 GbE	45	Nó de 10/25 GbE
46	Nó de 10/25 GbE	46	Nó de 10/25 GbE
47	Nó de 10/25 GbE	47	Nó de 10/25 GbE
48	Nó de 10/25 GbE	48	Nó de 10/25 GbE

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
49	Nó de 40/100 GbE	49	Nó de 40/100 GbE
50	Nó de 40/100 GbE	50	Nó de 40/100 GbE
51	Nó de 40/100 GbE	51	Nó de 40/100 GbE
52	Nó de 40/100 GbE	52	Nó de 40/100 GbE
53	Nó de 40/100 GbE	53	Nó de 40/100 GbE
54	Nó de 40/100 GbE	54	Nó de 40/100 GbE
55	Nó de 40/100 GbE	55	Nó de 40/100 GbE
56	Nó de 40/100 GbE	56	Nó de 40/100 GbE
57	Nó de 40/100 GbE	57	Nó de 40/100 GbE
58	Nó de 40/100 GbE	58	Nó de 40/100 GbE
59	Nó de 40/100 GbE	59	Nó de 40/100 GbE
60	Nó de 40/100 GbE	60	Nó de 40/100 GbE
61	Nó de 40/100 GbE	61	Nó de 40/100 GbE
62	Nó de 40/100 GbE	62	Nó de 40/100 GbE
63	Nó de 40/100 GbE	63	Nó de 40/100 GbE
64	Nó de 40/100 GbE	64	Nó de 40/100 GbE
65	100 GbE ISL para a porta 65 do switch B.	65	100 GbE ISL para switch A porta 65
66	100 GbE ISL para a porta 66 do switch B.	66	100 GbE ISL para switch A porta 65

Folha de cálculo de cablagem em branco

Você pode usar a Planilha de cabeamento em branco para documentar as plataformas compatíveis como nós em um cluster. A seção *conexões de cluster suportadas* da "Hardware Universe" define as portas de cluster usadas pela plataforma.

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
Porta do switch	Uso de nó/porta	Porta do switch	Uso de nó/porta
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	

Interrutor do cluster A		Interrutor B do grupo de instrumentos	
65	ISL para a porta 65 do interrutor B.	65	ISL para mudar A porta 65
66	ISL para a porta 66 do interrutor B.	66	ISL para mudar A porta 66

O que vem a seguir

"Instale o interrutor" .

Instalar o switch de cluster 92300YC

Siga este procedimento para configurar e configurar o switch Cisco Nexus 92300YC.

Antes de começar

Certifique-se de que tem o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no site de instalação para baixar as versões NX-os e Reference Configuration File (RCF) aplicáveis.
- Versão NX-os aplicável, transferida a partir da "Transferência do software Cisco" página.
- Licenças aplicáveis, informações de rede e configuração e cabos.
- Concluído"fichas de trabalho de cablagem" .
- RCFs de rede de cluster e rede de gerenciamento NetApp aplicáveis baixados do site de suporte da NetApp em "mysupport.NetApp.com". Todos os switches de rede e rede de gerenciamento de cluster Cisco chegam com a configuração padrão de fábrica do Cisco. Esses switches também têm a versão atual do software NX-os, mas não têm os RCFs carregados.
- "Documentação necessária do switch e do ONTAP" .

Passos

1. Coloque em rack os switches e controladores de rede de gerenciamento e rede de cluster.

Se você está instalando o…	Então…
Cisco Nexus 92300YC em um gabinete de sistema NetApp	Consulte o guia _Instalação de um switch de cluster Cisco Nexus 92300YC e painel de passagem em um gabinete NetApp para obter instruções sobre como instalar o switch em um gabinete NetApp .
Equipamento em um rack Telco	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração do NetApp.

2. Faça o cabeamento dos switches de rede e rede de gerenciamento do cluster para os controladores usando as planilhas de cabeamento concluídas.
3. Ligue a rede do cluster e os controladores e switches de rede de gerenciamento.

O que se segue?

Opcionalmente, você pode"instalar um switch Cisco Nexus 3223C em um gabinete NetApp" . Caso contrário,

vá para"Revise o cabeamento e a configuração" .

Instalar um switch de cluster Cisco Nexus 92300YC em um gabinete NetApp

Dependendo da sua configuração, pode ser necessário instalar o switch de cluster Cisco Nexus 92300YC e o painel de passagem em um gabinete NetApp com os suportes padrão incluídos com o switch.

Antes de começar

- Os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança no"Guia de instalação de hardware do Cisco Nexus 9000 Series" .
- Para cada interrutor, os oito parafusos 10-32 ou 12-24 e as porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiros e traseiros do armário.
- Kit de trilho padrão Cisco para instalar o interrutor em um gabinete NetApp.

> Os cabos de ligação em ponte não estão incluídos no kit de passagem e devem ser incluídos com os switches. Se eles não foram enviados com os switches, você pode encomendá-los da NetApp (código de peça X1558A-R6).

Passos

1. Instale o painel obturador de passagem no gabinete NetApp.

   O kit de painel de passagem está disponível na NetApp (código de peça X8784-R6).

   O kit do painel de passagem do NetApp contém o seguinte hardware:

   - Um painel obturador de passagem
   - Quatro parafusos 10-32 x .75
   - Quatro porcas de freio 10-32

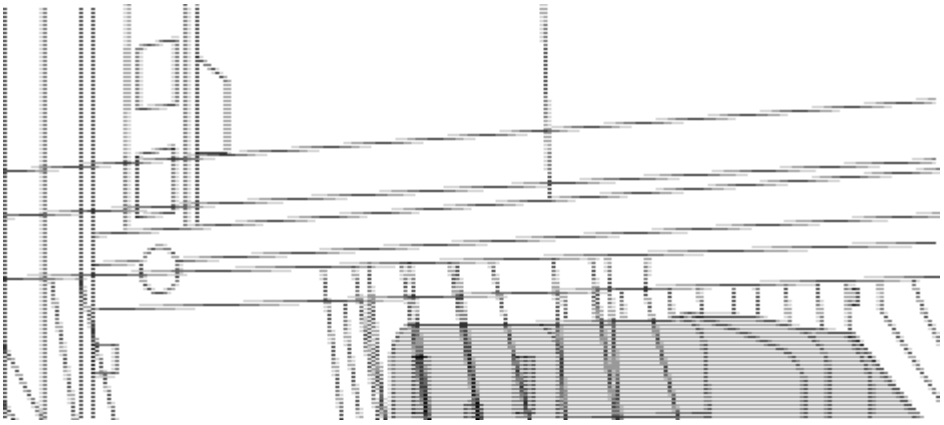
     i. Determine a localização vertical dos interrutores e do painel obturador no gabinete.

     Neste procedimento, o painel obturador será instalado em U40.

     ii. Instale duas porcas de mola em cada lado nos orifícios quadrados apropriados para os trilhos dianteiros do gabinete.

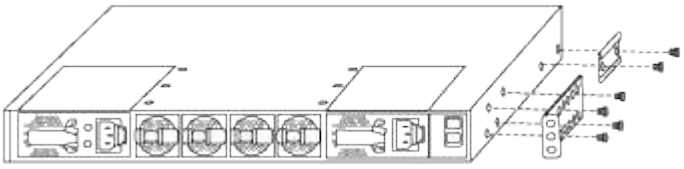
     iii. Centralize o painel verticalmente para evitar a intrusão no espaço adjacente do rack e, em seguida, aperte os parafusos.

     iv. Insira os conetores fêmea de ambos os cabos de ligação em ponte de 48 polegadas a partir da parte traseira do painel e através do conjunto da escova.

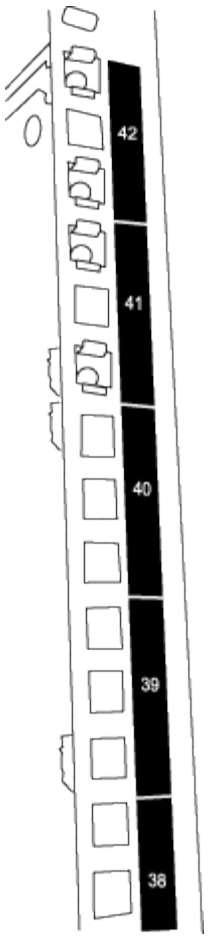


(1) conetor fêmea do cabo de ligação em ponte.

1. Instale os suportes de montagem em rack no chassi do switch Nexus 92300YC.
   a. Posicione um suporte dianteiro de montagem em rack em um lado do chassi do interrutor de modo que a orelha de montagem fique alinhada com a placa frontal do chassi (no lado da PSU ou do ventilador) e, em seguida, use quatro parafusos M4 para prender o suporte ao chassi.



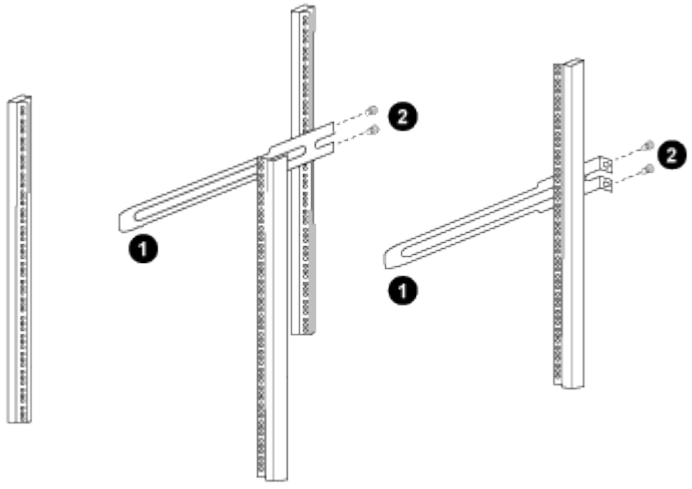
   b. Repita o passo 2a com o outro suporte de montagem em rack dianteiro do outro lado do interrutor.
   c. Instale o suporte traseiro do suporte do suporte do rack no chassis do interrutor.
   d. Repita o passo 2c com o outro suporte de montagem em rack traseiro do outro lado do interrutor.
2. Instale as porcas de mola nas localizações dos orifícios quadrados para os quatro postes IEA.



Os dois switches 92300YC sempre serão montados no 2U superior do gabinete RU41 e 42.

3. Instale os trilhos deslizantes no gabinete.

   a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste esquerdo traseiro, insira os parafusos com o tipo de rosca correspondente e aperte os parafusos com os dedos.



*(1) ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos no rack.*__(2) aperte os parafusos dos trilhos deslizantes nos postes do gabinete._

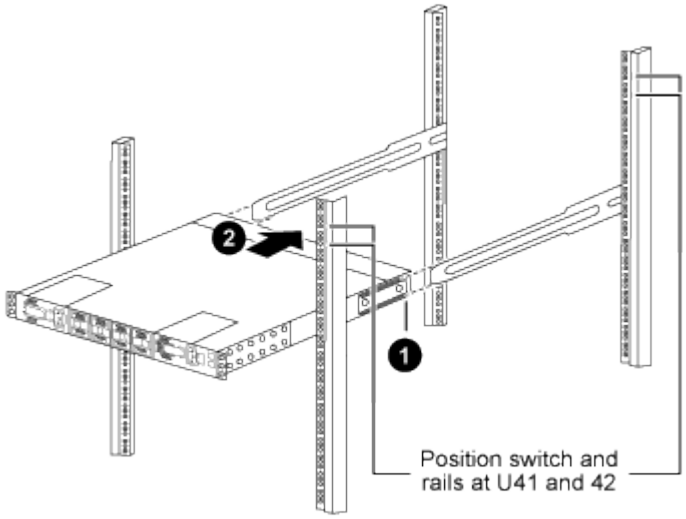
   a. Repita o passo 4a para a coluna traseira do lado direito.

b. Repita as etapas 4a e 4b nos RU41 locais do gabinete.

4. Instale o interrutor no gabinete.

> Este passo requer duas pessoas: Uma pessoa para apoiar o interrutor da frente e outra para guiar o interrutor para os trilhos deslizantes traseiros.

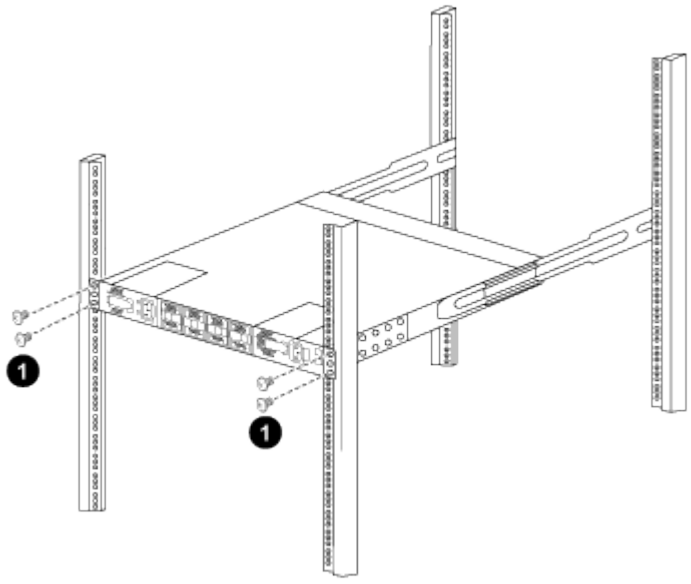
a. Posicione a parte traseira do interrutor em RU41.



(1) à medida que o chassis é empurrado para os postes traseiros, alinhe as duas guias de montagem em rack traseiras com os trilhos deslizantes.

(2) deslize suavemente o interrutor até que os suportes de montagem em rack dianteiros estejam alinhados com os postes dianteiros.

b. Ligue o interrutor ao armário.



(1) com uma pessoa segurando a frente do nível do chassi, a outra pessoa deve apertar totalmente os quatro parafusos traseiros aos postes do gabinete.

a. Com o chassis agora suportado sem assistência, aperte totalmente os parafusos dianteiros nos

postes.

b. Repita os passos 5a a 5c para o segundo interrutor na localização RU42.

> Ao utilizar o interrutor totalmente instalado como suporte, não é necessário manter a frente do segundo interrutor durante o processo de instalação.

5. Quando os switches estiverem instalados, conete os cabos de ligação em ponte às entradas de energia do switch.
6. Ligue as fichas macho de ambos os cabos de ligação em ponte às tomadas PDU mais próximas disponíveis.

> Para manter a redundância, os dois cabos devem ser conetados a diferentes PDUs.

7. Conecte a porta de gerenciamento em cada switch 92300YC a qualquer um dos switches de gerenciamento (se solicitado) ou conecte-os diretamente à sua rede de gerenciamento.

   A porta de gerenciamento é a porta superior direita localizada no lado da PSU do switch. O cabo CAT6 para cada switch precisa ser encaminhado através do painel de passagem depois que os switches são instalados para se conetar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração

Antes de configurar o switch Cisco 92300YC, revise as seguintes considerações.

Suporte para portas NVIDIA CX6, CX6-DX e CX7 Ethernet

Se estiver conetando uma porta de switch a um controlador ONTAP usando as portas de NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), é necessário codificar a velocidade da porta do switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte o "Hardware Universe" para obter mais informações sobre portas do switch.

Configurar o software

Fluxo de trabalho de instalação de software para switches de cluster Cisco Nexus 92300YC

Para instalar e configurar o software para um switch Cisco Nexus 92300YC e instalar ou

atualizar o arquivo de configuração de referência (RCF), siga estas etapas:

1. **"Configure o interrutor"**

Configurar o switch de cluster 92300YC.

2. **"Prepare-se para instalar o software NX-os e o RCF"**

O software Cisco NX-OS e os arquivos de configuração de referência (RCFs) devem ser instalados nos switches de cluster Cisco 92300YC.

3. **"Instale ou atualize o software NX-os"**

Baixe e instale ou atualize o software NX-OS no switch de cluster Cisco 392300YC.

4. **"Instale o RCF"**

Instale o RCF após configurar o switch Cisco 92300YC pela primeira vez.

5. **"Verifique a configuração do SSH"**

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

Configure o switch Cisco Nexus 92300YC

Siga este procedimento para configurar e configurar o switch Cisco Nexus 92300YC.

Passos

1. Conete a porta serial a um host ou porta serial.
2. Conete a porta de gerenciamento (no lado que não seja da porta do switch) à mesma rede onde o servidor SFTP está localizado.
3. No console, defina as configurações de série do lado do host:
   - 9600 baud
   - 8 bits de dados
   - 1 bit de paragem
   - paridade: nenhuma
   - controle de fluxo: nenhum
4. Ao inicializar pela primeira vez ou reiniciar depois de apagar a configuração em execução, o switch Nexus 92300YC é loop em um ciclo de inicialização. Interrompa este ciclo digitando **yes** para cancelar o fornecimento automático de energia.

   É apresentada a configuração da conta de administrador do sistema.

Mostrar exemplo

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: y
Disabling POAP.......Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

          ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Digite **y** para aplicar o padrão de senha segura:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Introduza e confirme a palavra-passe do administrador do utilizador:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Digite **yes** para entrar na caixa de diálogo Configuração básica do sistema.

Mostrar exemplo

```
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 Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 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.

Would you like to enter the basic configuration dialog (yes/no):
```

8. Criar outra conta de login:

```
Create another login account (yes/no) [n]:
```

9. Configurar strings de comunidade SNMP somente leitura e leitura-escrita:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Configure o nome do switch de cluster:

```
Enter the switch name : cs2
```

11. Configure a interface de gerenciamento fora da banda:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Configurar opções IP avançadas:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configurar serviços Telnet:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configurar serviços SSH e chaves SSH:

```
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]: 2048
```

15. Configurar outras definições:

```
Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L2]: L2

  Configure default switchport interface state (shut/noshut) [noshut]:
noshut

  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Confirme as informações do interrutor e guarde a configuração:

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

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

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

O que se segue?

"Prepare-se para instalar o software NX-os e o RCF".

Preparar para instalar o software NX-os e o ficheiro de configuração de referência (RCF)

Antes de instalar o software NX-os e o ficheiro de configuração de referência (RCF), siga este procedimento.

Antes de começar

Certifique-se de que tem o seguinte:

- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- Guias de software e atualização apropriados, disponíveis em "Switches Cisco Nexus 9000 Series".

Sobre os exemplos

Os exemplos neste procedimento usam dois nós. Esses nós usam duas portas de interconexão de cluster

10GbE `e0a` e `e0b`. Consulte "Hardware Universe" para verificar as portas de cluster corretas nas suas plataformas.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `node1` e `node2`.
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos Cisco Nexus 9000 Series switches; os comandos ONTAP são usados, a menos que indicado de outra forma. As saídas de comando podem variar dependendo de diferentes versões do ONTAP.

Passos

1. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   `set -privilege advanced`

   (`*>`É apresentado o aviso avançado).

2. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=xh`

   onde *x* é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   cluster1:> **system node autosupport invoke -node * -type all -message
   MAINT=2h**
   ```

3. Exiba quantas interfaces de interconexão de cluster são configuradas em cada nó para cada switch de interconexão de cluster: `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

 Node/      Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C92300YC
            e0b    cs2                       Eth1/2            N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C92300YC
            e0b    cs2                       Eth1/1            N9K-
C92300YC

4 entries were displayed.
```

4. Verifique o status administrativo ou operacional de cada interface de cluster.
   a. Exibir os atributos da porta de rede: `network port show –ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node2
                                                        Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node1
                                                        Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Exibir informações sobre os LIFs: `network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------ ------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o comando de reversão automática está ativado em todas as LIFs do cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

O que se segue?

"Instale o software NX-os".

Instale o software NX-os

Siga este procedimento para instalar o software NX-os no switch Nexus 92300YC.

NX-os é um sistema operacional de rede para a série Nexus de switches Ethernet e MDS série de switches de rede de área de armazenamento Fibre Channel (FC) fornecidos pela Cisco Systems.

Rever os requisitos

Portas e conexões de nós compatíveis

- Os ISLs (Inter-Switch Links) suportados para os switches Nexus 92300YC são as portas 1/65 e 1/66.
- As conexões de nós suportadas pelos switches Nexus 92300YC são as portas 1/1 a 1/66.

Antes de começar

Certifique-se de que tem o seguinte:

- Software NetApp Cisco NX-os aplicável para os seus comutadores a partir do site de suporte da NetApp, disponível em "mysupport.NetApp.com"
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- "Página do switch Ethernet Cisco". Consulte a tabela de compatibilidade do switch para ver as versões suportadas do ONTAP e NX-os.

Instale o software

Os exemplos neste procedimento usam dois nós, mas você pode ter até 24 nós em um cluster.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches Nexus 92300YC são `cs1` e `cs2`.
- O exemplo usado neste procedimento inicia a atualização no segundo switch, **CS2**.
- Os nomes de LIF do cluster são `node1_clus1` e `node1_clus2` para node1 `node2_clus1` e e `node2_clus2` node2.
- O nome do IPspace é `Cluster`.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster em cada nó são nomeadas e `e0a` `e0b`.

  Consulte a "*Hardware Universe*" para obter as portas de cluster reais suportadas na sua plataforma.

Passos

1. Conete o switch de cluster à rede de gerenciamento.
2. Use o `ping` comando para verificar a conetividade com o servidor que hospeda o software NX-os e o RCF.

   Mostrar exemplo

   Este exemplo verifica se o switch pode alcançar o servidor no endereço IP 172.19.2.1:

   ```
   cs2# ping 172.19.2.1
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Copie o software NX-os e as imagens EPLD para o switch Nexus 92300YC.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verifique a versão em execução do software NX-os:

   ```
   show version
   ```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.31
  NXOS: version 9.2(1)
  BIOS compile time:  05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time:  7/17/2018 16:00:00 [07/18/2018 00:21:19]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Instale a imagem NX-os.

   Instalar o arquivo de imagem faz com que ele seja carregado toda vez que o switch é reinicializado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.9.2.2.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS



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



Images will be upgraded according to following table:

Module   Image         Running-Version(pri:alt            New-
Version         Upg-Required
------  --------  ------------------------------------
------------------  ------------
  1       nxos                                   9.2(1)
9.2(2)         yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)       yes
```

```
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
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

Finishing the upgrade, switch will reboot in 10 seconds.
```

6. Verifique a nova versão do software NX-os depois que o switch reiniciar:

```
show version
```

Mostrar exemplo

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)

Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

```
  Reason: Reset due to upgrade
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

7. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI FPGA                               0x7
IO FPGA                               0x17
MI FPGA2                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2

cs2# install epld bootflash:n9000-epld.9.2.2.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.

Mostrar exemplo

```
cs2# *show version module 1 epld*

EPLD Device                          Version
---------------------------------------
MI FPGA                               0x7
IO FPGA                               0x19
MI FPGA2                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2
GEM FPGA                              0x2
```

O que se segue?

"Instale o ficheiro de configuração de referência"

Instalar o ficheiro de configuração de referência (RCF)

Você pode instalar o RCF depois de configurar o switch Nexus 92300YC pela primeira vez. Você também pode usar este procedimento para atualizar sua versão RCF.

Consulte o artigo da base de dados de Conhecimento "Como limpar a configuração em um switch de interconexão Cisco, mantendo a conetividade remota"para obter mais informações ao instalar ou atualizar o RCF.

Sobre esta tarefa

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `node1` e `node2`.
- Os nomes de LIF do cluster são `node1_clus1`, `node1_clus2`, `node2_clus1`, `node2_clus2` e .
- O `cluster1::*>` prompt indica o nome do cluster.

- O procedimento requer a utilização de ambos os comandos ONTAP e "Switches Cisco Nexus 9000 Series"; os comandos ONTAP são utilizados, salvo indicação em contrário.
- Antes de executar este procedimento, certifique-se de que tem uma cópia de segurança atual da configuração do comutador.
- Não é necessária qualquer ligação entre interrutores (ISL) operacional durante este procedimento. Isso é feito por design porque as alterações na versão do RCF podem afetar temporariamente a conetividade do ISL. Para garantir operações de cluster sem interrupções, o procedimento a seguir migra todas as LIFs de cluster para o switch de parceiro operacional enquanto executa as etapas no switch de destino.

Passos

1. Exiba as portas do cluster em cada nó conetado aos switches do cluster:
`network device-discovery show`

Mostrar exemplo

```
cluster1::*> *network device-discovery show*
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/1     N9K-
C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/2     N9K-
C92300YC
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta de cluster.
   a. Verifique se todas as portas do cluster estão ativas com um status de integridade:
   `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> *network port show -ipspace Cluster*

Node: node1

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: node2

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
cluster1::*>
```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta inicial:
`network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> *network interface show -vserver Cluster*
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            node1_clus1        up/up      169.254.3.4/23    node1
e0c     true
            node1_clus2        up/up      169.254.3.5/23    node1
e0d     true
            node2_clus1        up/up      169.254.3.8/23    node2
e0c     true
            node2_clus2        up/up      169.254.3.9/23    node2
e0d     true
cluster1::*>
```

c. Verifique se o cluster exibe informações para ambos os switches do cluster:
`system cluster-switch show -is-monitoring-enabled-operational true`

Mostrar exemplo

```
cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                        Type               Address
Model
---------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.233.205.92
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                           cluster-network    10.233.205.93
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Desative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

4. No switch de cluster CS2, encerre as portas conetadas às portas de cluster dos nós.

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Verifique se as portas de cluster migraram para as portas hospedadas no switch de cluster CS1. Isso pode levar alguns segundos.
   `network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> *network interface show -vserver Cluster*
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            node1_clus1       up/up      169.254.3.4/23     node1
e0c     true
            node1_clus2       up/up      169.254.3.5/23     node1
e0c     false
            node2_clus1       up/up      169.254.3.8/23     node2
e0c     true
            node2_clus2       up/up      169.254.3.9/23     node2
e0c     false
cluster1::*>
```

6. Verifique se o cluster está em bom estado:
`cluster show`

Mostrar exemplo

```
cluster1::*> *cluster show*
Node           Health  Eligibility   Epsilon
-------------- ------- ------------  -------
node1          true    true          false
node2          true    true          false
cluster1::*>
```

7. Se você ainda não fez isso, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

`show running-config`

8. Limpe a configuração no interrutor CS2 e execute uma configuração básica.

> Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e executar a configuração básica. Você deve estar conetado à porta do console serial do switch para configurar o switch novamente.

a. Limpar a configuração:

Mostrar exemplo

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n)  [n]  y
```

b. Execute uma reinicialização do switch:

Mostrar exemplo

```
(cs2)# reload

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

9. Copie o RCF para o flash de inicialização do switch CS2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Switches Cisco Nexus 9000 Series" nos guias.

   Este exemplo mostra TFTP sendo usado para copiar um RCF para o flash de inicialização no switch CS2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. Aplique o RCF baixado anteriormente ao flash de inicialização.

    Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Switches Cisco Nexus 9000 Series" nos guias.

Este exemplo mostra o arquivo RCF `Nexus_92300YC_RCF_v1.0.2.txt` sendo instalado no switch CS2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands

Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits)......
generated ecdsa key

Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a
single
 host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
 Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
 have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...
Copy complete.
```

11. Verifique no switch se o RCF foi mesclado com êxito:

```
show running-config
```

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*
```

Ao aplicar o RCF pela primeira vez, a mensagem **ERROR: Failed to write VSH commands** é esperada e pode ser ignorada.

1. Verifique se o arquivo RCF é a versão mais recente correta:

`show running-config`

Quando verificar a saída para verificar se tem o RCF correto, certifique-se de que as seguintes informações estão corretas:

- O banner RCF
- As configurações de nó e porta
- Personalizações

  A saída varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para ver se há alterações específicas ao RCF que você instalou.

2. Reaplique quaisquer personalizações anteriores à configuração do switch. "Analise as considerações sobre cabeamento e configuração"Consulte para obter detalhes sobre quaisquer alterações adicionais necessárias.
3. Depois de verificar se as versões do RCF e as configurações do switch estão corretas, copie o arquivo running-config para o arquivo startup-config.

   Para obter mais informações sobre comandos Cisco, consulte o guia apropriado "Switches Cisco Nexus 9000 Series" nos guias.

```
cs2# copy running-config startup-config
[] 100% Copy complete
```

4. Interrutor de reinicialização CS2. Você pode ignorar os eventos "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
cs2# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Verifique a integridade das portas do cluster no cluster.

   a. Verifique se as portas e0d estão ativas e íntegras em todos os nós do cluster:
   `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> *network port show -ipspace Cluster*

Node: node1

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

b. Verifique a integridade do switch a partir do cluster (isso pode não mostrar o switch CS2, uma vez que LIFs não são homed em e0d).

Mostrar exemplo

```
cluster1::*> *network device-discovery show -protocol cdp*
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1
N9K-C92300YC
            e0b    cs2                       Ethernet1/1
N9K-C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/2
N9K-C92300YC
            e0b    cs2                       Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Você pode observar a seguinte saída no console do switch CS1, dependendo da versão RCF previamente carregada no switch

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

6. No switch de cluster CS1, encerre as portas conetadas às portas de cluster dos nós.

   O exemplo a seguir usa a saída de exemplo de interface do passo 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

7. Verifique se os LIFs de cluster migraram para as portas hospedadas no switch CS2. Isso pode levar alguns segundos. `network interface show -vserver Cluster`

   Mostrar exemplo

```
cluster1::*> *network interface show -vserver Cluster*
            Logical          Status     Network            Current
Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node
Port    Home
----------- ---------------- ---------- ------------------
----------------- ------- ----
Cluster
            node1_clus1      up/up      169.254.3.4/23     node1
e0d     false
            node1_clus2      up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1      up/up      169.254.3.8/23     node2
e0d     false
            node2_clus2      up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

8. Verifique se o cluster está em bom estado:
   `cluster show`

Mostrar exemplo

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-------------- -------- ------------- -------
node1          true     true          false
node2          true     true          false
cluster1::*>
```

9. Repita os passos 7 a 14 no interrutor CS1.
10. Ative a reversão automática nos LIFs do cluster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

11. Interrutor de reinicialização CS1. Você faz isso para acionar os LIFs do cluster para reverter para suas portas domésticas. Você pode ignorar os eventos "portas de cluster para baixo" relatados nos nós enquanto o switch é reinicializado.

```
cs1# reload
This command will reboot the system. (y/n)?  [n] y
```

12. Verifique se as portas do switch conetadas às portas do cluster estão ativadas.

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1       eth  access up      none
10G(D) --
Ethernet1/2      1       eth  access up      none
10G(D) --
Ethernet1/3      1       eth  trunk  up      none
100G(D) --
Ethernet1/4      1       eth  trunk  up      none
100G(D) --
.
.
```

13. Verifique se o ISL entre CS1 e CS2 está funcional:
`show port-channel summary`

Mostrar exemplo

```
cs1# *show port-channel summary*
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
cs1#
```

14. Verifique se os LIFs do cluster reverteram para sua porta inicial:
`network interface show -vserver Cluster`

Mostrar exemplo

```
cluster1::*> *network interface show -vserver Cluster*
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
------------ ------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/23     node1
e0d     true
            node1_clus2   up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1   up/up      169.254.3.8/23     node2
e0d     true
            node2_clus2   up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

15. Verifique se o cluster está em bom estado:
`cluster show`

Mostrar exemplo

```
cluster1::*> *cluster show*
Node           Health  Eligibility   Epsilon
-------------- ------- ------------- -------
node1          true    true          false
node2          true    true          false
```

16. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

O que se segue?

"Verifique a configuração do SSH".

Verifique a configuração da SSH

Se você estiver usando os recursos CSHM (Ethernet Switch Health Monitor) e coleta de logs, verifique se as chaves SSH e SSH estão habilitadas nos switches de cluster.

Passos

1. Verifique se o SSH está ativado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verifique se as chaves SSH estão ativadas:

   `show ssh key`

   Mostrar exemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Ao ativar o FIPS, você deve alterar o número de bits para 256 na central usando o comando `ssh key ecdsa 256 force`. "Configurar a segurança da rede usando o FIPS"Consulte para obter mais detalhes.

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migrar switches

Migre para um cluster comutado de dois nós com um switch Cisco Nexus 92300YC

Se você tiver um ambiente de cluster *sem switch* de dois nós, poderá migrar para um ambiente de cluster *comutado* de dois nós usando os switches Cisco Nexus 92300YC para permitir que você escale além de dois nós no cluster.

O procedimento usado depende se você tem duas portas de rede de cluster dedicadas em cada controlador ou uma única porta de cluster em cada controlador. O processo documentado funciona para todos os nós que usam portas óticas ou twinax, mas não é suportado neste switch se os nós estiverem usando portas integradas 10Gb BASE-T RJ45 para as portas de cluster-rede.

A maioria dos sistemas requer duas portas de rede de cluster dedicadas em cada controlador.

Após a conclusão da migração, talvez seja necessário instalar o arquivo de configuração necessário para dar suporte ao Cluster Switch Health Monitor (CSHM) para switches de cluster 92300YC. Ver "Monitoramento de integridade do switch (CSHM)" .

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

Para uma configuração sem switch de dois nós, certifique-se de que:

- A configuração sem switch de dois nós está corretamente configurada e funcionando.
- Os nós estão executando o ONTAP 9.6 e posterior.
- Todas as portas de cluster estão no estado **up**.
- Todas as interfaces lógicas de cluster (LIFs) estão no estado **up** e em suas portas domésticas.

Para a configuração do switch Cisco Nexus 92300YC:

- Ambos os switches têm conetividade de rede de gerenciamento.
- Existe acesso à consola aos interrutores do cluster.
- As conexões de switch nó a nó Nexus 92300YC e switch a switch usam cabos twinax ou de fibra.

  "Hardware Universe - interrutores" contém mais informações sobre cabeamento.

- Os cabos ISL (Inter-Switch Link) são conetados às portas 1/65 e 1/66 em ambos os switches 92300YC.
- A personalização inicial de ambos os 92300YC switches está concluída. Para que:
  - Os switches 92300YC estão executando a versão mais recente do software

◦ Arquivos de Configuração de Referência (RCFs) são aplicados aos switches qualquer personalização de site, como SMTP, SNMP e SSH, é configurada nos novos switches.

Migrar o switch

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches 92300YC são CS1 e CS2.
- Os nomes dos SVMs do cluster são node1 e node2.
- Os nomes dos LIFs são node1_clus1 e node1_clus2 no nó 1 e node2_clus1 e node2_clus2 no nó 2 respetivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas do cluster usadas neste procedimento são e0a e e0b.

  "Hardware Universe" contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

2. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde x é a duração da janela de manutenção em horas.

   A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   Mostrar exemplo

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar cabos e portas

1. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster CS1 e CS2.

   Não deve desativar as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 64 voltadas para o nó estão desativadas no switch CS1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e/1-64
cs1(config-if-range)# shutdown
```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches 92300YC CS1 e CS2 estão acima nas portas 1/65 e 1/66:

   ```
   show port-channel summary
   ```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS1:

```
cs1# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

O exemplo a seguir mostra que as portas ISL estão acima no interrutor CS2 :

E

```
(cs2)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

3. Exibir a lista de dispositivos vizinhos:

   ```
   show cdp neighbors
   ```

   Este comando fornece informações sobre os dispositivos que estão conetados ao sistema.

Mostrar exemplo

O exemplo a seguir lista os dispositivos vizinhos no switch CS1:

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

O exemplo a seguir lista os dispositivos vizinhos no switch CS2:

E

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1(FDO220329KU)    Eth1/65        177    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)    Eth1/66        177    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

4. Verifique se todas as portas do cluster estão ativas:

```
network port show -ipspace Cluster
```

Cada porta deve ser exibida para `Link` e saudável para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node2

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

5. Verifique se todas as LIFs de cluster estão ativas e operacionais:

   `network interface show -vserver Cluster`

   Cada LIF de cluster deve exibir true para `Is Home` e ter um `Status Admin/Oper` de up/up

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

   `network interface show -vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. Desconete o cabo da porta de cluster e0a no node1 e conete o e0a à porta 1 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches 92300YC.

O "*Hardware Universe - switches*" contém mais informações sobre cabeamento.

8. Desconete o cabo da porta de cluster e0a no node2 e conete o e0a à porta 2 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches 92300YC.
9. Habilite todas as portas voltadas para o nó no switch de cluster CS1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/64 estão ativadas no switch CS1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

10. Verifique se todas as LIFs do cluster estão ativas, operacionais e exibidas como verdadeiras para `Is Home`:

```
network interface show -vserver Cluster
```

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> network interface show -vserver Cluster

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node         Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1        e0a
true
         node1_clus2  up/up      169.254.49.125/16  node1        e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2        e0a
true
         node2_clus2  up/up      169.254.19.183/16  node2        e0b
true

4 entries were displayed.
```

11. Exibir informações sobre o status dos nós no cluster:

    ```
    cluster show
    ```

    Mostrar exemplo

    O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

    ```
    cluster1::*> cluster show

    Node                 Health  Eligibility   Epsilon
    -------------------- ------- ------------  ------------
    node1                true    true          false
    node2                true    true          false

    2 entries were displayed.
    ```

12. Desconete o cabo da porta de cluster e0b no node1 e conete o e0b à porta 1 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches 92300YC.
13. Desconete o cabo da porta de cluster e0b no node2 e conete o e0b à porta 2 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches 92300YC.
14. Habilite todas as portas voltadas para o nó no switch de cluster CS2.

    Mostrar exemplo

    O exemplo a seguir mostra que as portas 1/1 a 1/64 estão ativadas no switch CS2:

    ```
    cs2# config
    Enter configuration commands, one per line. End with CNTL/Z.
    cs2(config)# interface e1/1-64
    cs2(config-if-range)# no shutdown
    ```

Etapa 3: Verifique a configuração

1. Verifique se todas as portas do cluster estão ativas:

    ```
    network port show -ipspace Cluster
    ```

Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão em node1 e node2:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.
```

2. Verifique se todas as interfaces exibem verdadeiro para `Is Home`:

   `network interface show -vserver Cluster`

   Isso pode levar vários minutos para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão em node1 e node2 e que `Is Home` os resultados são verdadeiros:

```
cluster1::*> network interface show -vserver Cluster

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true

4 entries were displayed.
```

3. Verifique se ambos os nós têm uma conexão com cada switch:

   `show cdp neighbors`

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
(cs1)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0a
node2               Eth1/2         133    H         FAS2980
e0a
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4


(cs2)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0b
node2               Eth1/2         133    H         FAS2980
e0b
cs1(FDO220329KU)
                    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

4. Exiba informações sobre os dispositivos de rede descobertos no cluster:

   `network device-discovery show -protocol cdp`

   Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.
```

5. Verifique se as definições estão desativadas:

   `network options switchless-cluster show`

   Pode demorar vários minutos para o comando ser concluído. Aguarde até que o anúncio "3 minutos de duração expire".

   Mostrar exemplo

   A saída falsa no exemplo a seguir mostra que as configurações estão desativadas:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

6. Verifique o status dos membros do nó no cluster:

   `cluster show`

Mostrar exemplo

O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

7. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local

Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Mostrar exemplo

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Migre de um switch Cisco para um switch Cisco Nexus 92300YC

Você pode migrar os switches de cluster Cisco mais antigos sem interrupções para um cluster ONTAP para os switches de rede de cluster Cisco Nexus 92300YC.

Após a conclusão da migração, talvez seja necessário instalar o arquivo de configuração necessário para dar suporte ao Cluster Switch Health Monitor (CSHM) para switches de cluster 92300YC. Ver "Monitoramento de integridade do switch (CSHM)" .

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um cluster existente totalmente funcional.
- Conectividade de 10 GbE e 40 GbE de nós para switches de cluster Nexus 92300YC.
- Todas as portas de cluster estão no estado up para garantir operações ininterruptas.
- Versão adequada do NX-os e arquivo de configuração de referência (RCF) instalados nos switches de cluster Nexus 92300YC.
- Um cluster NetApp redundante e totalmente funcional usando ambos os switches Cisco mais antigos.
- Conetividade de gerenciamento e acesso ao console aos switches Cisco mais antigos e aos novos switches.
- Todas as LIFs de cluster no estado up com os LIFs de cluster estão em suas portas residenciais.
- Portas ISL ativadas e cabeadas entre os switches Cisco mais antigos e entre os novos switches.

Migrar o switch

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os switches de cluster Cisco Nexus 5596UP existentes são C1 e C2.
- Os novos switches de cluster Nexus 92300YC são CS1 e CS2.
- Os nós são node1 e node2.
- Os LIFs de cluster são node1_clus1 e node1_clus2 no nó 1 e node2_clus1 e node2_clus2 no nó 2, respetivamente.
- O interrutor C2 é substituído primeiro pelo interrutor CS2 e, em seguida, o interrutor C1 é substituído pelo interrutor CS1.
  - Um ISL temporário é construído em CS1 conetando C1 a CS1.
  - O cabeamento entre os nós e o C2 é desconetado do C2 e reconetado ao CS2.
  - O cabeamento entre os nós e o C1 é desconetado do C1 e reconetado ao CS1.
  - A ISL temporária entre C1 e CS1 é então removida.

Portas usadas para conexões

- Algumas das portas são configuradas nos switches Nexus 92300YC para serem executadas a 10 GbE ou 40 GbE.
- Os switches de cluster usam as seguintes portas para conexões com nós:

- Portas E1/1-48 (10/25 GbE), E1/49-64 (40/100 GbE): Nexus 92300YC
- Portas E1/1-40 (10 GbE): Nexus 5596UP
- Portas E1/1-32 (10 GbE): Nexus 5020
- Portas E1/1-12, E2/1-6 (10 GbE): Nexus 5010 com módulo de expansão

- Os switches do cluster usam as seguintes portas ISL (Inter-Switch Link):
  - Portas E1/65-66 (100 GbE): Nexus 92300YC
  - Portas E1/41-48 (10 GbE): Nexus 5596UP
  - Portas E1/33-40 (10 GbE): Nexus 5020
  - Portas E1/13-20 (10 GbE): Nexus 5010
- "Hardware Universe - interrutores" contém informações sobre cabeamento suportado para todos os switches de cluster.
- As versões ONTAP e NX-os suportadas neste procedimento estão "Switches Ethernet Cisco" na página.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

2. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   onde x é a duração da janela de manutenção em horas.

   A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   Mostrar exemplo

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

3. Verifique se a reversão automática está ativada em todas as LIFs do cluster:

   ```
   network interface show -vserver Cluster -fields auto-revert
   ```

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

4. Determine o status administrativo ou operacional de cada interface de cluster:

   Cada porta deve ser exibida para `Link` e saudável para `Health Status`.

   a. Exibir os atributos da porta de rede:

      `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.
```

b. Exibir informações sobre as interfaces lógicas e seus nós iniciais designados:

`network interface show -vserver Cluster`

Cada LIF deve exibir up/up para `Status Admin/Oper` e true para `Is Home`.

Mostrar exemplo

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

5. Verifique se as portas de cluster em cada nó estão conetadas aos switches de cluster existentes da seguinte maneira (da perspetiva dos nós) usando o comando:

   `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    c1                        0/2               N5K-
C5596UP
            e0b    c2                        0/2               N5K-
C5596UP
node1      /cdp
            e0a    c1                        0/1               N5K-
C5596UP
            e0b    c2                        0/1               N5K-
C5596UP

4 entries were displayed.
```

6. Verifique se as portas e os switches do cluster estão conetados da seguinte maneira (da perspetiva dos switches) usando o comando:

   `show cdp neighbors`

Mostrar exemplo

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
c2(FOX2025GEFC)     Eth1/41        179    S I s     N5K-C5596UP
Eth1/41

c2(FOX2025GEFC)     Eth1/42        175    S I s     N5K-C5596UP
Eth1/42

c2(FOX2025GEFC)     Eth1/43        179    S I s     N5K-C5596UP
Eth1/43

c2(FOX2025GEFC)     Eth1/44        175    S I s     N5K-C5596UP
Eth1/44

c2(FOX2025GEFC)     Eth1/45        179    S I s     N5K-C5596UP
Eth1/45

c2(FOX2025GEFC)     Eth1/46        179    S I s     N5K-C5596UP
Eth1/46

c2(FOX2025GEFC)     Eth1/47        175    S I s     N5K-C5596UP
Eth1/47

c2(FOX2025GEFC)     Eth1/48        179    S I s     N5K-C5596UP
Eth1/48

Total entries displayed: 10


c2# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1         124    H         FAS2750
e0b
node2                 Eth1/2         124    H         FAS2750
e0b
c1(FOX2025GEEX)     Eth1/41        175    S I s     N5K-C5596UP
Eth1/41

c1(FOX2025GEEX)     Eth1/42        175    S I s     N5K-C5596UP
Eth1/42

c1(FOX2025GEEX)     Eth1/43        175    S I s     N5K-C5596UP
Eth1/43

c1(FOX2025GEEX)     Eth1/44        175    S I s     N5K-C5596UP
Eth1/44

c1(FOX2025GEEX)     Eth1/45        175    S I s     N5K-C5596UP
Eth1/45

c1(FOX2025GEEX)     Eth1/46        175    S I s     N5K-C5596UP
Eth1/46

c1(FOX2025GEEX)     Eth1/47        176    S I s     N5K-C5596UP
Eth1/47

c1(FOX2025GEEX)     Eth1/48        176    S I s     N5K-C5596UP
Eth1/48
```

7. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Etapa 2: Configurar cabos e portas

1. Configure um ISL temporário em cs1on portas E1/41-48, entre C1 e CS1.

Mostrar exemplo

O exemplo a seguir mostra como o novo ISL é configurado no C1 e CS1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP
and Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range)# no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config)# interface port-channel 101
cs1(config-if)# switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

2. Remova os cabos ISL das portas E1/41-48 do C2 e conete os cabos às portas E1/41-48 do CS1.
3. Verifique se as portas ISL e o canal de porta estão operacionais conetando C1 e CS1:

   ```
   show port-channel summary
   ```

Mostrar exemplo

O exemplo a seguir mostra o comando Cisco show port-channel summary que está sendo usado para verificar se as portas ISL estão operacionais em C1 e CS1:

```
c1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)


cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
101   Po101(SU)   Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)
```

4. Para node1, desconete o cabo de E1/1 no C2 e conete o cabo a E1/1 no CS2, usando o cabeamento apropriado suportado pelo Nexus 92300YC.
5. Para node2, desconete o cabo de E1/2 no C2 e conete o cabo a E1/2 no CS2, usando o cabeamento apropriado suportado pelo Nexus 92300YC.
6. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol cdp`

   Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    c1                        0/2               N5K-
C5596UP
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    c1                        0/1               N5K-
C5596UP
            e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.
```

7. Para node1, desconete o cabo de E1/1 no C1 e conete o cabo a E1/1 no CS1, usando o cabeamento apropriado suportado pelo Nexus 92300YC.
8. Para node2, desconete o cabo de E1/2 no C1 e conete o cabo a E1/2 no CS1, usando o cabeamento apropriado suportado pelo Nexus 92300YC.
9. As portas do cluster em cada nó agora são conetadas aos switches do cluster da seguinte maneira, da perspetiva dos nós:

   `network device-discovery show -protocol cdp`

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC
4 entries were displayed.
```

10. Elimine o ISL temporário entre CS1 e C1.

Mostrar exemplo

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

Passo 3: Conclua a migração

1. Verifique a configuração final do cluster:

   `network port show -ipspace Cluster`

   Cada porta deve ser exibida para `Link` e saudável para `Health Status`.

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
```

```
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.


cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------ ----------------
----------------
node2      /cdp
            e0a    cs1                      0/2               N9K-
C92300YC
            e0b    cs2                      0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                      0/1               N9K-
C92300YC
            e0b    cs2                      0/1               N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
cs2(FDO220329V5)    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
```

```
cs2(FDO220329V5)    Eth1/66         179    R S I s   N9K-C92300YC
Eth1/66


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0b
node2               Eth1/2         124    H         FAS2750
e0b
cs1(FDO220329KU)
                    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

2. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=END`

   Mostrar exemplo

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

2. Altere o nível de privilégio de volta para admin:

   `set -privilege admin`

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os interrutores

Substitua um switch Cisco Nexus 92300YC

Substituir um switch Nexus 92300YC defeituoso em uma rede de cluster é um procedimento sem interrupções (NDU).

Rever os requisitos

Antes de começar

Antes de efetuar a substituição do interrutor, certifique-se de que:

- No cluster existente e infra-estrutura de rede:
  - O cluster existente é verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
  - Todas as portas do cluster estão ativas.
  - Todas as interfaces lógicas de cluster (LIFs) estão ativas e em suas portas domésticas.
  - O comando ping-cluster -nó node1 do cluster do ONTAP deve indicar que a conetividade básica e a comunicação maior do que a PMTU são bem-sucedidas em todos os caminhos.
- Para o interrutor de substituição do Nexus 92300YC:
  - A conetividade de rede de gerenciamento no switch de substituição está funcional.
  - O acesso do console ao interrutor de substituição está no lugar.
  - As conexões de nó são as portas 1/1 a 1/64.
  - Todas as portas ISL (Inter-Switch Link) estão desativadas nas portas 1/65 e 1/66.
  - O arquivo de configuração de referência desejado (RCF) e o switch de imagem do sistema operacional NX-os são carregados no switch.
  - A personalização inicial do interrutor está completa, como detalhado em: "Configure o switch Cisco Nexus 92300YC".

    Quaisquer personalizações de sites anteriores, como STP, SNMP e SSH, são copiadas para o novo switch.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desativar a criação de casos durante a manutenção. Consulte este artigo da base de dados de Conhecimento "SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para obter mais detalhes.
- Ativar o registo de sessão para quaisquer sessões CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" neste artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os nomes dos switches Nexus 92300YC existentes são CS1 e CS2.
- O nome do novo switch Nexus 92300YC é newcs2.
- Os nomes dos nós são node1 e node2.
- As portas de cluster em cada nó são denominadas e0a e e0b.
- Os nomes de LIF do cluster são node1_clus1 e node1_clus2 para node1, e node2_clus1 e node2_clus2 para node2.
- O prompt para alterações em todos os nós de cluster é cluster1::*>

Sobre esta tarefa

Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.

O procedimento a seguir é baseado na seguinte topologia de rede de cluster:

Mostrar topologia

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
4 entries were displayed.



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C92300YC
            e0b    cs2                       Eth1/2            N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C92300YC
            e0b    cs2                       Eth1/1            N9K-
C92300YC
4 entries were displayed.



cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2(FDO220329V5)   Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
cs2(FDO220329V5)   Eth1/66        176    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

Passo 1: Prepare-se para a substituição

1. Instale o RCF e a imagem apropriados no interrutor, newcs2, e faça os preparativos necessários para o local.

   Se necessário, verifique, baixe e instale as versões apropriadas do software RCF e NX-os para o novo switch. Se tiver verificado que o novo switch está corretamente configurado e não precisa de atualizações para o software RCF e NX-os, avance para o passo 2.

   a. Vá para a página *NetApp Cluster and Management Network switches Referência Configuração do arquivo Descrição* no site de suporte da NetApp.

   b. Clique no link para a *Cluster Network and Management Network Compatibility Matrix* e observe a versão necessária do software do switch.

   c. Clique na seta de volta do seu navegador para retornar à página **Descrição**, clique em **CONTINUAR**, aceite o contrato de licença e, em seguida, vá para a página **Download**.

   d. Siga as etapas na página Download para baixar os arquivos RCF e NX-os corretos para a versão do software ONTAP que você está instalando.

2. No novo switch, faça login como administrador e encerre todas as portas que serão conetadas às interfaces do cluster de nós (portas 1/1 a 1/64).

   Se o interrutor que está a substituir não estiver funcional e estiver desligado, avance para o passo 4. As LIFs nos nós de cluster já devem ter falhado para a outra porta de cluster para cada nó.

Mostrar exemplo

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Verifique se todas as LIFs do cluster têm a reversão automática ativada:

   `network interface show -vserver Cluster -fields auto-revert`

Mostrar exemplo

```
cluster1::> network interface show -vserver Cluster -fields auto-
revert

             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Etapa 2: Configurar cabos e portas

1. Desligue as portas ISL 1/65 e 1/66 no switch Nexus 92300YC CS1:

   Mostrar exemplo

   ```
   cs1# configure
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/65-66
   cs1(config-if-range)# shutdown
   cs1(config-if-range)#
   ```

2. Remova todos os cabos do switch Nexus 92300YC CS2 e conete-os às mesmas portas do switch Nexus 92300YC newcs2.
3. Abra as portas ISLs 1/65 e 1/66 entre os switches CS1 e newcs2 e verifique o status da operação do canal da porta.

   O Canal de porta deve indicar PO1(SU) e os portos Membros devem indicar eth1/65(P) e eth1/66(P).

Mostrar exemplo

Este exemplo ativa as portas ISL 1/65 e 1/66 e apresenta o resumo do canal da porta no interrutor CS1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)

cs1(config-if-range)#
```

4. Verifique se a porta e0b está ativa em todos os nós:

   `network port show ipspace Cluster`

Mostrar exemplo

A saída deve ser semelhante ao seguinte:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/auto   -
false

4 entries were displayed.
```

5. No mesmo nó usado na etapa anterior, reverta o LIF do cluster associado à porta na etapa anterior usando o comando de reversão da interface de rede.

Mostrar exemplo

Neste exemplo, LIF node1_clus2 no node1 é revertido com sucesso se o valor Casa for verdadeiro e a porta for e0b.

Os comandos a seguir retornam LIF `node1_clus2` `node1` à porta inicial `e0a` e exibem informações sobre os LIFs em ambos os nós. Abrir o primeiro nó é bem-sucedido se a coluna is Home for verdadeira para ambas as interfaces de cluster e elas mostrarem as atribuições de porta corretas, neste `e0a` exemplo e `e0b` no node1.

```
cluster1::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Exibir informações sobre os nós em um cluster:

`cluster show`

Mostrar exemplo

Este exemplo mostra que a integridade do nó para node1 e node2 neste cluster é verdadeira:

```
cluster1::*> cluster show

Node          Health  Eligibility
------------- ------- ------------
node1         false   true
node2         true    true
```

7. Verifique se todas as portas de cluster físico estão ativas:

   `network port show ipspace Cluster`

   Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e0a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e0b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

Ignore
                                                       Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e0a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up    9000  auto/10000
healthy  false

4 entries were displayed.
```

Passo 3: Conclua o procedimento

1. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Confirme a seguinte configuração de rede de cluster:

```
network port show
```

Mostrar exemplo

```
cluster1::*> network port show -ipspace Cluster
Node: node1

Ignore
                                        Speed(Mbps)            Health
Health
Port      IPspace     Broadcast Domain Link MTU   Admin/Oper  Status
Status
--------- ----------- ---------------- ---- ----- -----------
-------- ------
e0a       Cluster     Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster     Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                         Speed(Mbps)           Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000 auto/10000
healthy  false

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

cluster1::> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    newcs2                    0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    newcs2                    0/1               N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     N9K-C92300YC
```

```
Eth1/66


Total entries displayed: 4


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e0b
node2              Eth1/2         124    H           FAS2980
e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

O que se segue?

"Configurar o monitoramento de integridade do switch".

Substitua os switches de cluster Cisco Nexus 92300YC por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver

executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

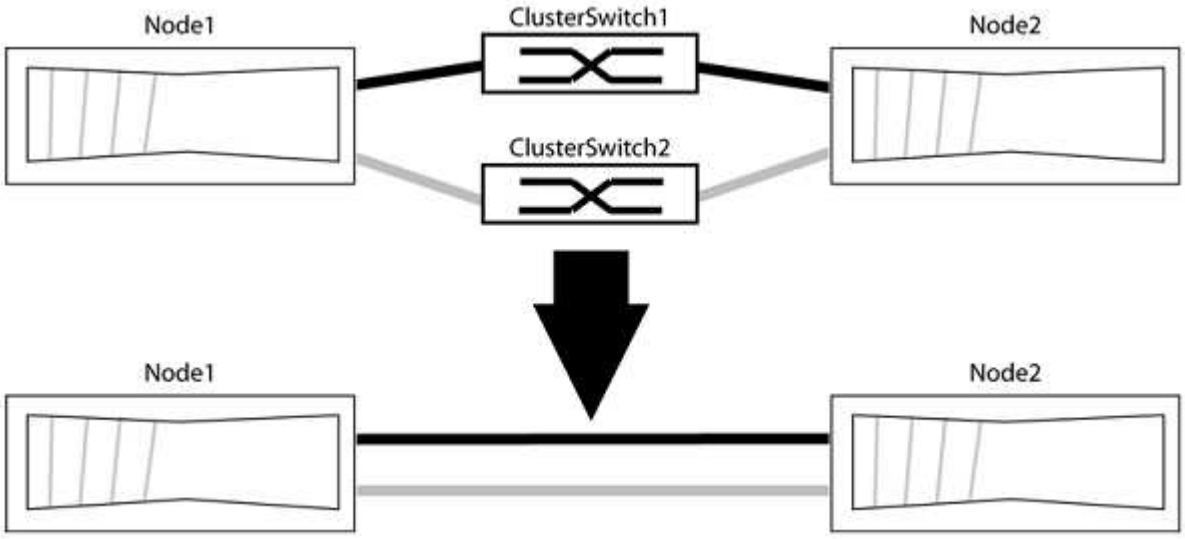
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

`network options detect-switchless-cluster show`

Mostrar exemplo

A saída de exemplo a seguir mostra se a opção está ativada.

```
cluster::*> network options detect-switchless-cluster show
   (network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=<number_of_hours>h`

   `h`onde está a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico desta tarefa de manutenção para que possa suprimir a criação automática de casos durante a janela de manutenção.

   No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

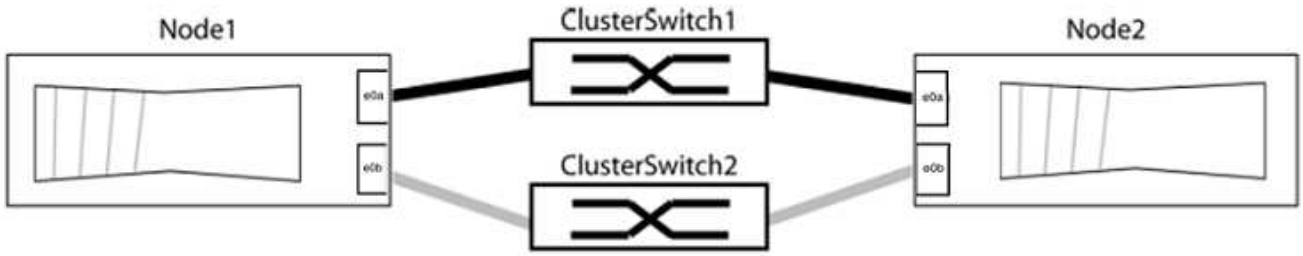
   Mostrar exemplo

   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-cisco-92300/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

```
network interface show -vserver Cluster -fields is-home
```

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

```
network interface revert -vserver Cluster -lif *
```

4. Desativar a reversão automática para as LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

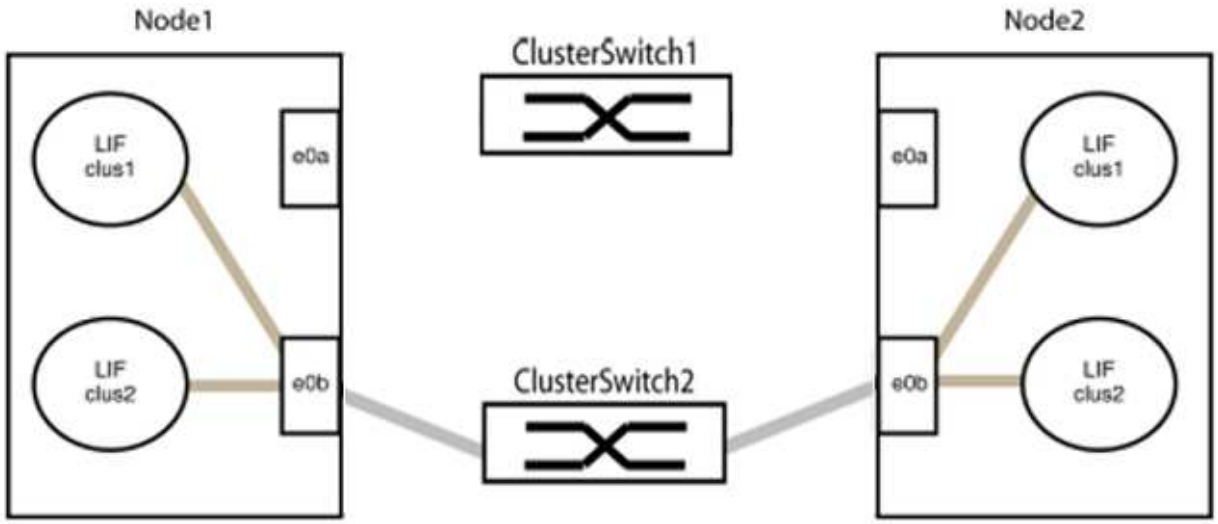
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   > Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

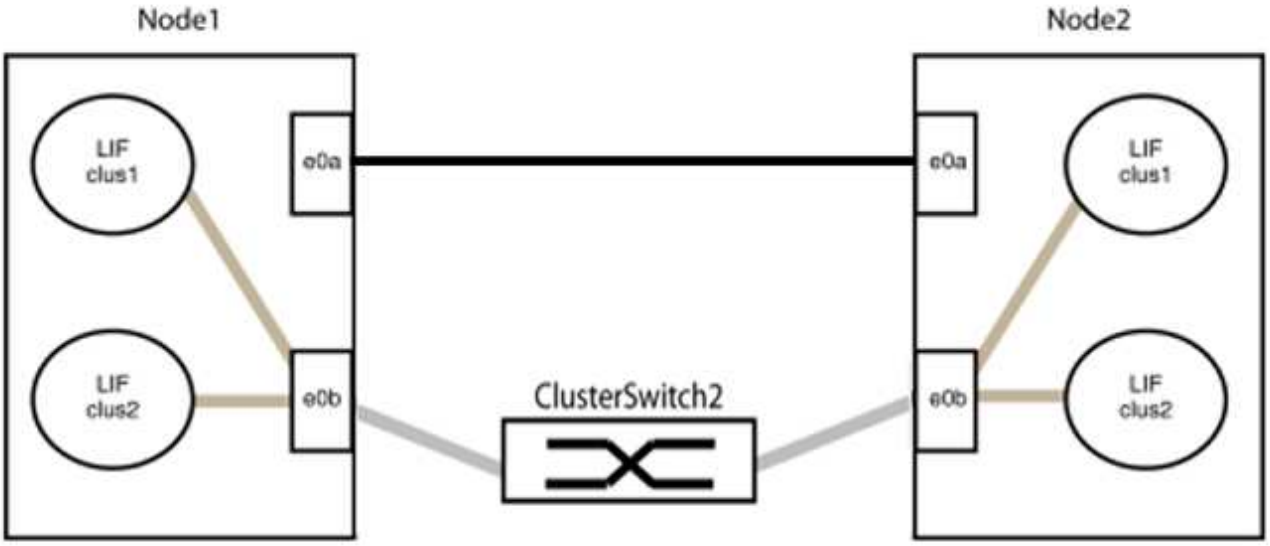
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

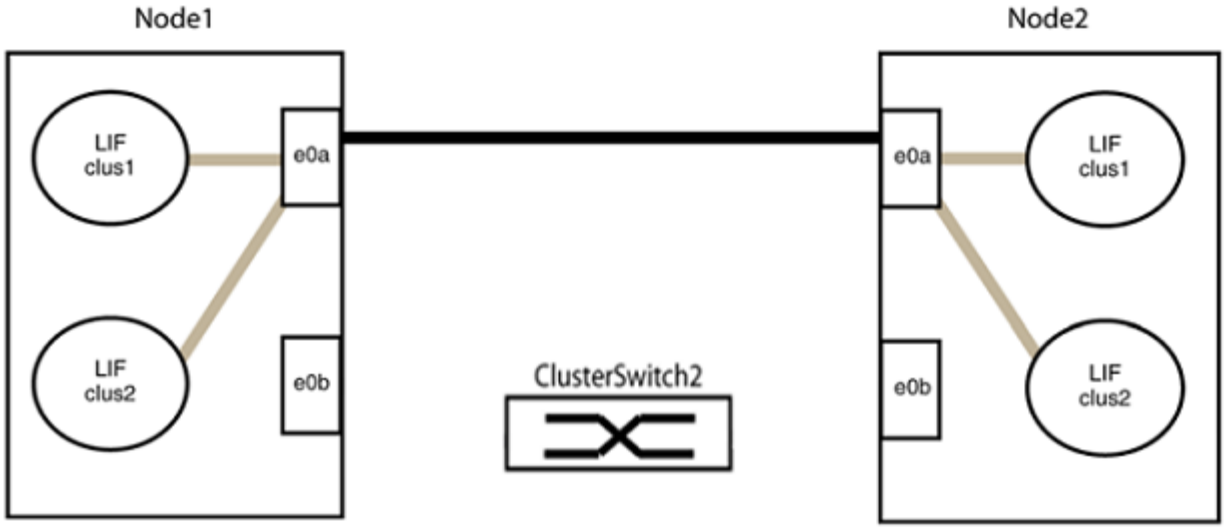
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

NetApp CN1610

Visão geral da instalação e configuração dos switches NetApp CN1610

O CN1610 é um switch de camada 2 gerenciado de alta largura de banda que fornece portas SFP (Small Form-factor Pluggable Plus) de 16 10 Gigabit.

O switch inclui fontes de alimentação redundantes e bandejas de ventiladores que suportam hot swap para alta disponibilidade. Este switch 1U pode ser instalado em um gabinete de sistema NetApp 42U padrão de 19 polegadas ou em um gabinete de terceiros.

O switch oferece suporte ao gerenciamento local por meio da porta do console ou do gerenciamento remoto usando Telnet ou SSH por meio de uma conexão de rede. O CN1610 inclui uma porta de gerenciamento dedicada Ethernet RJ45 de 1 Gigabit para gerenciamento de switch fora da banda. Você pode gerenciar o switch inserindo comandos na interface de linha de comando (CLI) ou usando um sistema de gerenciamento de rede baseado em SNMP (NMS).

Instalar e configurar o fluxo de trabalho para os switches NetApp CN1610

Para instalar e configurar um switch NetApp CN1610 em sistemas que executam o ONTAP, siga estas etapas:

1. "Instale o hardware"
2. "Instale o software FASTPATH"
3. "Instale o ficheiro de configuração de referência"

   Se os switches estiverem executando o ONTAP 8.3.1 ou posterior, siga as instruções em "Instale FASTPATH e RCFs nos switches que executam o ONTAP 8.3.1 e posterior."

4. "Configure o interrutor"

Requisitos de documentação para switches NetApp CN1610

Para a instalação e manutenção do switch NetApp CN1610, certifique-se de revisar toda a documentação recomendada.

Título do documento	Descrição
"Guia de Instalação DO 1g"	Uma visão geral dos recursos de hardware e software do switch CN1601 e do processo de instalação.
"Guia de Instalação DO 10g"	Uma visão geral dos recursos de hardware e software do switch CN1610 e descreve os recursos para instalar o switch e acessar a CLI.
"Guia de configuração e configuração do switch CN1601 e CN1610"	Detalhes sobre como configurar o hardware e o software do switch para o ambiente do cluster.
CN1601 Guia do Administrador do comutador	Fornece exemplos de como usar o switch CN1601 em uma rede típica. • "Guia do administrador" • "Guia do administrador, versão 1,1.x.x" • "Guia do administrador, versão 1,2.x.x"

Título do documento	Descrição
Referência de comando CLI do comutador de rede CN1610	Fornece informações detalhadas sobre os comandos de interface de linha de comando (CLI) que você usa para configurar o software CN1601. • "Referência do comando" • "Referência de comando, versão 1,1.x.x" • "Referência de comando, versão 1,2.x.x"

Instalar e configurar

Instale o hardware do switch NetApp CN1610

Para instalar o hardware do switch NetApp CN1610, use as instruções em um dos guias a seguir.

- "Guia de Instalação DO 1g".

  Uma visão geral dos recursos de hardware e software do switch CN1601 e do processo de instalação.

- "Guia de Instalação DO 10g"

  Uma visão geral dos recursos de hardware e software do switch CN1610 e descreve os recursos para instalar o switch e acessar a CLI.

Instale o software FASTPATH

Quando você instala o software FASTPATH em seus switches NetApp, você deve começar a atualização com o segundo switch, *CS2*.

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede de cluster (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster configuradas.
- Todas as interfaces lógicas de cluster (LIFs) configuradas (não devem ter sido migradas).
- Um caminho de comunicação bem-sucedido: O comando ONTAP (privilégio: Avançado) `cluster ping-cluster -node node1` deve indicar que `larger than PMTU communication` é bem-sucedido em todos os caminhos.
- Uma versão suportada do FASTPATH e ONTAP.

  Certifique-se de consultar a tabela de compatibilidade de switch na "Switches NetApp CN1601 e CN1610"

página para as versões FASTPATH e ONTAP suportadas.

Instale o FASTPATH

O procedimento a seguir usa a sintaxe Clustered Data ONTAP 8.2. Como resultado, o SVM de cluster, os nomes de LIF e a saída de CLI são diferentes dos do Data ONTAP 8.3.

Pode haver dependências de comando entre sintaxe de comando nas versões RCF e FASTPATH.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os dois switches NetApp são CS1 e CS2.
- Os dois LIFs de cluster são clus1 e clus2.
- Os VServers são VS1 e VS2.
- O `cluster::*>` prompt indica o nome do cluster.
- As portas de cluster em cada nó são denominadas e1a e E2A.

  "Hardware Universe" tem mais informações sobre as portas de cluster reais que são suportadas na sua plataforma.

- Os ISLs (Inter-Switch Links) suportados são as portas 0/13 a 0/16.
- As conexões de nós suportadas são as portas 0/1 a 0/12.

Etapa 1: Migrar cluster

1. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all - message MAINT=xh`

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

2. Faça login no switch como admin. Por padrão, não há senha. No `(cs2) #` prompt, digite o `enable` comando. Novamente, não há senha por padrão. Isso lhe dá acesso ao modo EXEC privilegiado, que permite configurar a interface de rede.

   Mostrar exemplo

   ```
   (cs2) # enable
   Password (Enter)
   (cs2) #
   ```

3. No console de cada nó, migre clus2 para a porta e1a:

`network interface migrate`

Mostrar exemplo

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2
-destnode node2 -dest-port e1a
```

4. No console de cada nó, verifique se a migração ocorreu:

   `network interface show`

   O exemplo a seguir mostra que o clus2 migrou para a porta e1a em ambos os nós:

   Mostrar exemplo

```
cluster::*> network interface show -role cluster

         Logical    Status     Network         Current  Current  Is
Vserver  Interface  Admin/Open Address/Mask    Node     Port     Home
-------- ---------- ---------- --------------- -------- -------  ----
vs1
         clus1      up/up      10.10.10.1/16   node1    e1a      true
         clus2      up/up      10.10.10.2/16   node1    e1a
false
vs2
         clus1      up/up      10.10.10.1/16   node2    e1a      true
         clus2      up/up      10.10.10.2/16   node2    e1a
false
```

Passo 2: Instale o software FASTPATH

1. Encerre a porta E2A do cluster em ambos os nós:

   `network port modify`

Mostrar exemplo

O exemplo a seguir mostra a porta E2A sendo fechada em ambos os nós:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

2. Verifique se a porta E2A está desligada em ambos os nós:

`network port show`

Mostrar exemplo

```
cluster::*> network port show -role cluster

                                  Auto-Negot  Duplex      Speed
(Mbps)
Node   Port Role     Link MTU    Admin/Oper  Admin/Oper  Admin/Oper
------ ---- -------- ---- -----  ----------  ----------
------------
node1
       e1a  cluster  up   9000   true/true   full/full   auto/10000
       e2a  cluster  down 9000   true/true   full/full   auto/10000
node2
       e1a  cluster  up   9000   true/true   full/full   auto/10000
       e2a  cluster  down 9000   true/true   full/full   auto/10000
```

3. Desligue as portas ISL (Inter-Switch Link) no CS1, o interrutor NetApp ativo:

Mostrar exemplo

```
(cs1) # configure
(cs1)(config) # interface 0/13-0/16
(cs1)(Interface 0/13-0/16) # shutdown
(cs1)(Interface 0/13-0/16) # exit
(cs1)(config) # exit
```

4. Faça uma cópia de segurança da imagem ativa atual no CS2.

Mostrar exemplo

```
(cs2) # show bootvar

 Image Descriptions   .

  active:
  backup:

 Images currently available on Flash

--------------------------------------------------------------------
--
 unit        active       backup     current-active       next-
active
--------------------------------------------------------------------
--

    1        1.1.0.3      1.1.0.1          1.1.0.3           1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful

(cs2) #
```

5. Transfira o ficheiro de imagem para o interrutor.

   Copiar o arquivo de imagem para a imagem ativa significa que, quando você reiniciar, essa imagem estabelece a versão FASTPATH em execução. A imagem anterior permanece disponível como cópia de segurança.

Mostrar exemplo

```
(cs2) # copy tftp://10.0.0.1/NetApp_CN1610_1.1.0.5.stk active


Mode..................................... TFTP
Set Server IP............................ 10.0.0.1
Path..................................... ./
Filename................................. NetApp_CN1610_1.1.0.5.stk
Data Type................................ Code
Destination Filename..................... active

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


File transfer operation completed successfully.
```

6. Verifique a versão em execução do software FASTPATH.

   `show version`

Mostrar exemplo

```
(cs2) # show version

Switch: 1

System Description..................... Broadcom Scorpion 56820
                                        Development System - 16 TENGIG,
                                        1.1.0.3, Linux 2.6.21.7
Machine Type........................... Broadcom Scorpion 56820
                                        Development System - 16TENGIG
Machine Model.......................... BCM-56820
Serial Number.......................... 10611100004
FRU Number............................
Part Number............................ BCM56820
Maintenance Level...................... A
Manufacturer........................... 0xbc00
Burned In MAC Address.................. 00:A0:98:4B:A9:AA
Software Version....................... 1.1.0.3
Operating System....................... Linux 2.6.21.7
Network Processing Device.............. BCM56820_B0
Additional Packages.................... FASTPATH QOS
                                        FASTPATH IPv6 Management
```

7. Visualize as imagens de arranque para a configuração ativa e de cópia de segurança.

   `show bootvar`

Mostrar exemplo

```
(cs2) # show bootvar

Image Descriptions

 active :
 backup :

 Images currently available on Flash

--------------------------------------------------------------------
--
 unit        active       backup     current-active       next-
active
--------------------------------------------------------------------
--

    1        1.1.0.3      1.1.0.3          1.1.0.3           1.1.0.5
```

8. Reinicie o switch.

   `reload`

Mostrar exemplo

```
(cs2) # reload

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

System will now restart!
```

Passo 3: Valide a instalação

1. Faça login novamente e verifique a nova versão do software FASTPATH.

   `show version`

Mostrar exemplo

```
(cs2) # show version

Switch: 1

System Description..................... Broadcom Scorpion 56820
                                        Development System - 16
TENGIG,
                                        1.1.0.5, Linux 2.6.21.7
Machine Type........................... Broadcom Scorpion 56820
                                        Development System - 16TENGIG
Machine Model.......................... BCM-56820
Serial Number.......................... 10611100004
FRU Number............................
Part Number............................ BCM56820
Maintenance Level...................... A
Manufacturer........................... 0xbc00
Burned In MAC Address.................. 00:A0:98:4B:A9:AA
Software Version....................... 1.1.0.5
Operating System....................... Linux 2.6.21.7
Network Processing Device.............. BCM56820_B0
Additional Packages.................... FASTPATH QOS
                                        FASTPATH IPv6 Management
```

2. Abra as portas ISL no CS1, o interrutor ativo.

   `configure`

   Mostrar exemplo

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

3. Verifique se os ISLs estão operacionais:

   `show port-channel 3/1`

   O campo Estado da ligação deve `Up` indicar .

Mostrar exemplo

```
(cs2) # show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

4. Copie o `running-config` arquivo para o `startup-config` arquivo quando estiver satisfeito com as versões de software e as configurações de switch.

Mostrar exemplo

```
(cs2) # 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!
```

5. Ative a segunda porta do cluster, E2A, em cada nó:

`network port modify`

Mostrar exemplo

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin
true**
```

6. Reverter clus2 associado à porta E2A:

   `network interface revert`

   O LIF pode reverter automaticamente, dependendo da sua versão do software ONTAP.

   Mostrar exemplo

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

7. Verifique se o LIF está agora em (`true`casa) em ambos os nós:

   `network interface show -role cluster`

   Mostrar exemplo

```
cluster::*> network interface show -role cluster

          Logical    Status     Network         Current  Current Is
Vserver   Interface  Admin/Oper Address/Mask    Node     Port    Home
--------  ---------- ---------- --------------- -------- ------- ----
vs1
          clus1      up/up      10.10.10.1/24   node1    e1a     true
          clus2      up/up      10.10.10.2/24   node1    e2a     true
vs2
          clus1      up/up      10.10.10.1/24   node2    e1a     true
          clus2      up/up      10.10.10.2/24   node2    e2a     true
```

8. Exibir o status dos nós:

   `cluster show`

Mostrar exemplo

```
cluster::> cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
```

9. Repita as etapas anteriores para instalar o software FASTPATH no outro switch, CS1.
10. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Instale um ficheiro de configuração de referência num switch CN1610

Siga este procedimento para instalar um ficheiro de configuração de referência (RCF).

Antes de instalar um RCF, você deve primeiro migrar os LIFs do cluster para longe do switch CS2. Depois que o RCF é instalado e validado, os LIFs podem ser migrados de volta.

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede de cluster (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster configuradas.
- Todas as interfaces lógicas de cluster (LIFs) configuradas.
- Um caminho de comunicação bem-sucedido: O comando ONTAP (privilégio: Avançado) `cluster ping-cluster -node node1` deve indicar que `larger than PMTU communication` é bem-sucedido em todos os caminhos.
- Uma versão suportada do RCF e do ONTAP.

  Certifique-se de que consulta a tabela de compatibilidade de switch na "Switches NetApp CN1601 e CN1610" página para as versões RCF e ONTAP suportadas.

Instale o RCF

O procedimento a seguir usa a sintaxe Clustered Data ONTAP 8.2. Como resultado, o SVM de cluster, os nomes de LIF e a saída de CLI são diferentes dos do Data ONTAP 8.3.

Pode haver dependências de comando entre sintaxe de comando nas versões RCF e FASTPATH.

No RCF versão 1,2, o suporte para Telnet foi explicitamente desativado devido a problemas de segurança. Para evitar problemas de conetividade durante a instalação do RCF 1,2, verifique se o Secure Shell (SSH) está ativado. O "Guia do administrador do switch NetApp CN1610" tem mais informações sobre SSH.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os dois switches NetApp são CS1 e CS2.
- Os dois LIFs de cluster são clus1 e clus2.
- Os VServers são VS1 e VS2.
- O `cluster::*>` prompt indica o nome do cluster.
- As portas de cluster em cada nó são denominadas e1a e E2A.

  "Hardware Universe" tem mais informações sobre as portas de cluster reais que são suportadas na sua plataforma.

- Os ISLs (Inter-Switch Links) suportados são as portas 0/13 a 0/16.
- As conexões de nós suportadas são as portas 0/1 a 0/12.
- Uma versão suportada do FASTPATH, RCF e ONTAP.

  Certifique-se de consultar a tabela de compatibilidade de switch na "Switches NetApp CN1601 e CN1610" página para as versões FASTPATH, RCF e ONTAP suportadas.

Etapa 1: Migrar cluster

1. Guarde as informações de configuração do seu switch atual:

   `write memory`

   Mostrar exemplo

   O exemplo a seguir mostra a configuração atual do switch que está sendo salva (`startup-config`no arquivo de configuração de inicialização) no switch CS2:

   ```
   (cs2) # 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!
   ```

2. No console de cada nó, migre clus2 para a porta e1a:

`network interface migrate`

Mostrar exemplo

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-source-node node1 -destnode node1 -dest-port e1a

cluster::*> network interface migrate -vserver vs2 -lif clus2
-source-node node2 -destnode node2 -dest-port e1a
```

3. No console de cada nó, verifique se a migração ocorreu:

`network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra que o clus2 migrou para a porta e1a em ambos os nós:

```
cluster::*> network port show -role cluster
         clus1      up/up      10.10.10.1/16   node2    e1a     true
         clus2      up/up      10.10.10.2/16   node2    e1a
false
```

4. Encerre a porta E2A em ambos os nós:

`network port modify`

Mostrar exemplo

O exemplo a seguir mostra a porta E2A sendo fechada em ambos os nós:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

5. Verifique se a porta E2A está desligada em ambos os nós:

`network port show`

Mostrar exemplo

```
cluster::*> network port show -role cluster

                                   Auto-Negot  Duplex      Speed
(Mbps)
Node   Port   Role     Link MTU   Admin/Oper  Admin/Oper  Admin/Oper
------ ------ -------- ---- ----- ----------- ----------
-----------
node1
       e1a    cluster  up   9000  true/true   full/full   auto/10000
       e2a    cluster  down 9000  true/true   full/full   auto/10000
node2
       e1a    cluster  up   9000  true/true   full/full   auto/10000
       e2a    cluster  down 9000  true/true   full/full   auto/10000
```

6. Desligue as portas ISL no CS1, o interrutor NetApp ativo.

Mostrar exemplo

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

Passo 2: Instale o RCF

1. Copie o RCF para o interrutor.

> Você deve definir a `.scr` extensão como parte do nome do arquivo antes de chamar o script. Esta extensão é a extensão para o sistema operacional FASTPATH.

O switch validará o script automaticamente à medida que ele é baixado para o switch, e a saída irá para o console.

Mostrar exemplo

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr

[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

2. Verifique se o script foi baixado e salvo com o nome do arquivo que você deu.

Mostrar exemplo

```
(cs2) # script list
Configuration Script Name        Size(Bytes)
-------------------------------- -----------
running-config.scr               6960
CN1610_CS_RCF_v1.1.scr           2199

2 configuration script(s) found.
6038 Kbytes free.
```

3. Valide o script.

> O script é validado durante o download para verificar se cada linha é uma linha de comando de switch válida.

Mostrar exemplo

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

4. Aplique o script ao switch.

Mostrar exemplo

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

5. Verifique se suas alterações foram implementadas no switch.

```
(cs2) # show running-config
```

O exemplo exibe o `running-config` arquivo no switch. Você deve comparar o arquivo com o RCF para verificar se os parâmetros definidos são como você espera.

6. Salve as alterações.
7. Defina o `running-config` arquivo para ser o padrão.

Mostrar exemplo

```
(cs2) # 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.
```

8. Reinicie o switch e verifique se o `running-config` arquivo está correto.

Após a conclusão da reinicialização, você deve fazer login, exibir o `running-config` arquivo e procurar a descrição na interface 3/64, que é o rótulo da versão para o RCF.

Mostrar exemplo

```
(cs2) # reload

The system has unsaved changes.
Would you like to save them now? (y/n) y


Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

9. Abra as portas ISL no CS1, o interrutor ativo.

Mostrar exemplo

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

10. Verifique se os ISLs estão operacionais:

`show port-channel 3/1`

O campo Estado da ligação deve `Up` indicar .

Mostrar exemplo

```
(cs2) # show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

11. Abra a porta de cluster E2A em ambos os nós:

    `network port modify`

    Mostrar exemplo

    O exemplo a seguir mostra a porta E2A sendo criada em node1 e node2:

    ```
    cluster::*> network port modify -node node1 -port e2a -up-admin true
    cluster::*> network port modify -node node2 -port e2a -up-admin true
    ```

Passo 3: Valide a instalação

1. Verifique se a porta E2A está ativa em ambos os nós:

   `network port show -role cluster`

Mostrar exemplo

```
cluster::*> network port show -role cluster

                                  Auto-Negot  Duplex      Speed (Mbps)
Node   Port Role     Link MTU    Admin/Oper  Admin/Oper  Admin/Oper
------ ---- -------- ---- ----  ----------- ----------  ------------
node1
       e1a  cluster  up   9000  true/true   full/full   auto/10000
       e2a  cluster  up   9000  true/true   full/full   auto/10000
node2
       e1a  cluster  up   9000  true/true   full/full   auto/10000
       e2a  cluster  up   9000  true/true   full/full   auto/10000
```

2. Em ambos os nós, reverta clus2 que está associado à porta E2A:

   `network interface revert`

   O LIF pode reverter automaticamente, dependendo da sua versão do ONTAP.

   Mostrar exemplo

   ```
   cluster::*> network interface revert -vserver node1 -lif clus2
   cluster::*> network interface revert -vserver node2 -lif clus2
   ```

3. Verifique se o LIF está agora em (`true`casa) em ambos os nós:

   `network interface show -role cluster`

   Mostrar exemplo

   ```
   cluster::*> network interface show -role cluster

           Logical    Status     Network         Current  Current Is
   Vserver Interface  Admin/Oper Address/Mask    Node     Port    Home
   ------- ---------- ---------- --------------- -------- ------- ----
   vs1
           clus1      up/up      10.10.10.1/24   node1    e1a     true
           clus2      up/up      10.10.10.2/24   node1    e2a     true
   vs2
           clus1      up/up      10.10.10.1/24   node2    e1a     true
           clus2      up/up      10.10.10.2/24   node2    e2a     true
   ```

4. Exibir o status dos membros do nó:

   `cluster show`

   Mostrar exemplo

   ```
   cluster::> cluster show

   Node           Health  Eligibility
   -------------- ------- ------------
   node1
                  true    true
   node2
                  true    true
   ```

5. Copie o `running-config` arquivo para o `startup-config` arquivo quando estiver satisfeito com as versões de software e as configurações de switch.

   Mostrar exemplo

   ```
   (cs2) # 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!
   ```

6. Repita os passos anteriores para instalar o RCF no outro interrutor, CS1.

O que se segue?

"Configurar o monitoramento de integridade do switch"

Instale o software FASTPATH e os RCFs para o ONTAP 8.3.1 e posterior

Siga este procedimento para instalar o software FASTPATH e os RCFs para o ONTAP 8.3.1 e posterior.

As etapas de instalação são as mesmas para os switches de gerenciamento NetApp CN1601 e CN1610 switches de cluster que executam o ONTAP 8.3.1 ou posterior. No entanto, os dois modelos requerem software e RCFs diferentes.

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede de cluster (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster configuradas.
- Todas as interfaces lógicas de cluster (LIFs) configuradas (não devem ter sido migradas).
- Um caminho de comunicação bem-sucedido: O comando ONTAP (privilégio: Avançado) `cluster ping-cluster -node node1` deve indicar que `larger than PMTU communication` é bem-sucedido em todos os caminhos.
- Uma versão suportada do FASTPATH, RCF e ONTAP.

  Certifique-se de consultar a tabela de compatibilidade de switch na "Switches NetApp CN1601 e CN1610" página para as versões FASTPATH, RCF e ONTAP suportadas.

Instale o software FASTPATH

O procedimento a seguir usa a sintaxe Clustered Data ONTAP 8.2. Como resultado, o SVM de cluster, os nomes de LIF e a saída de CLI são diferentes dos do Data ONTAP 8.3.

Pode haver dependências de comando entre sintaxe de comando nas versões RCF e FASTPATH.

> No RCF versão 1,2, o suporte para Telnet foi explicitamente desativado devido a problemas de segurança. Para evitar problemas de conetividade durante a instalação do RCF 1,2, verifique se o Secure Shell (SSH) está ativado. O "Guia do administrador do switch NetApp CN1610" tem mais informações sobre SSH.

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de switch e nó:

- Os dois nomes de switch NetApp são CS1 e CS2.
- Os nomes da interface lógica de cluster (LIF) são node1_clus1 e node1_clus2 para node1 e node2_clus1 e node2_clus2 para node2. (Você pode ter até 24 nós em um cluster.)
- O nome da máquina virtual de storage (SVM) é Cluster.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster em cada nó são denominadas e0a e e0b.

  "Hardware Universe" tem mais informações sobre as portas de cluster reais que são suportadas na sua plataforma.

- Os ISLs (Inter-Switch Links) suportados são as portas 0/13 a 0/16.
- As conexões de nós suportadas são as portas 0/1 a 0/12.

Etapa 1: Migrar cluster

1. Exibir informações sobre as portas de rede no cluster:

   `network port show -ipspace cluster`

   Mostrar exemplo

   O exemplo a seguir mostra o tipo de saída do comando:

```
cluster1::> network port show -ipspace cluster
                                                                        Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
node2
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
4 entries were displayed.
```

2. Apresentar informações sobre os LIFs no cluster:

   `network interface show -role cluster`

Mostrar exemplo

O exemplo a seguir mostra as interfaces lógicas no cluster. Neste exemplo, o `-role` parâmetro exibe informações sobre os LIFs associados às portas de cluster:

```
cluster1::> network interface show -role cluster
  (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    10.254.66.82/16    node1
e0a     true
            node1_clus2  up/up    10.254.206.128/16  node1
e0b     true
            node2_clus1  up/up    10.254.48.152/16   node2
e0a     true
            node2_clus2  up/up    10.254.42.74/16    node2
e0b     true
4 entries were displayed.
```

3. Em cada nó respetivo, usando um LIF de gerenciamento de nós, migre node1_clus2 para e0a em node1 e node2_clus2 para e0a em node2:

   `network interface migrate`

   Você deve inserir os comandos nos consoles do controlador que possuem os respetivos LIFs de cluster.

   Mostrar exemplo

   ```
   cluster1::> network interface migrate -vserver Cluster -lif
   node1_clus2 -destination-node node1 -destination-port e0a
   cluster1::> network interface migrate -vserver Cluster -lif
   node2_clus2 -destination-node node2 -destination-port e0a
   ```

   Para esse comando, o nome do cluster diferencia maiúsculas de minúsculas e o comando deve ser executado em cada nó. Não é possível executar este comando no cluster geral LIF.

4. Verifique se a migração ocorreu usando o `network interface show` comando em um nó.

Mostrar exemplo

O exemplo a seguir mostra que o clus2 migrou para a porta e0a nos nós node1 e node2:

```
cluster1::> **network interface show -role cluster**
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    10.254.66.82/16   node1
e0a     true
            node1_clus2  up/up    10.254.206.128/16 node1
e0a     false
            node2_clus1  up/up    10.254.48.152/16  node2
e0a     true
            node2_clus2  up/up    10.254.42.74/16   node2
e0a     false
4 entries were displayed.
```

5. Altere o nível de privilégio para avançado, inserindo y quando solicitado a continuar:

   `set -privilege advanced`

   É apresentado o aviso avançado (*>).

6. Encerre a porta e0b do cluster em ambos os nós:

   `network port modify -node node_name -port port_name -up-admin false`

   Você deve inserir os comandos nos consoles do controlador que possuem os respetivos LIFs de cluster.

   Mostrar exemplo

   O exemplo a seguir mostra os comandos para encerrar a porta e0b em todos os nós:

   ```
   cluster1::*> network port modify -node node1 -port e0b -up-admin
   false
   cluster1::*> network port modify -node node2 -port e0b -up-admin
   false
   ```

7. Verifique se a porta e0b está desligada em ambos os nós:

```
network port show
```

Mostrar exemplo

```
cluster1::*> network port show -role cluster

                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          down     9000
auto/10000
node2
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          down     9000
auto/10000
4 entries were displayed.
```

8. Encerre as portas ISL (Inter-Switch Link) no CS1.

Mostrar exemplo

```
(cs1) #configure
(cs1) (Config)#interface 0/13-0/16
(cs1) (Interface 0/13-0/16)#shutdown
(cs1) (Interface 0/13-0/16)#exit
(cs1) (Config)#exit
```

9. Faça uma cópia de segurança da imagem ativa atual no CS2.

Mostrar exemplo

```
(cs2) # show bootvar

 Image Descriptions

 active :
 backup :


 Images currently available on Flash

--------------------------------------------------------------------
 unit      active      backup     current-active        next-active
--------------------------------------------------------------------

    1     1.1.0.5     1.1.0.3            1.1.0.5            1.1.0.5

(cs2) # copy active backup
Copying active to backup
Copy operation successful
```

Passo 2: Instale o software FASTPATH e RCF

1. Verifique a versão em execução do software FASTPATH.

Mostrar exemplo

```
(cs2) # show version

Switch: 1

System Description..............................  NetApp CN1610,
1.1.0.5, Linux
                                                   2.6.21.7
Machine Type....................................  NetApp CN1610
Machine Model...................................  CN1610
Serial Number...................................  20211200106
Burned In MAC Address...........................  00:A0:98:21:83:69
Software Version................................  1.1.0.5
Operating System................................  Linux 2.6.21.7
Network Processing Device.......................  BCM56820_B0
Part Number.....................................  111-00893

--More-- or (q)uit


Additional Packages.............................  FASTPATH QOS
                                                   FASTPATH IPv6
Management
```

2. Transfira o ficheiro de imagem para o interrutor.

   Copiar o arquivo de imagem para a imagem ativa significa que, quando você reiniciar, essa imagem estabelece a versão FASTPATH em execução. A imagem anterior permanece disponível como cópia de segurança.

Mostrar exemplo

```
(cs2) #copy
sftp://root@10.22.201.50//tftpboot/NetApp_CN1610_1.2.0.7.stk active
Remote Password:********

Mode..................................... SFTP
Set Server IP.................................. 10.22.201.50
Path..................................... /tftpboot/
Filename.....................................
NetApp_CN1610_1.2.0.7.stk
Data Type...................................... Code
Destination Filename........................... active

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


File transfer operation completed successfully.
```

3. Confirme as versões de imagem de arranque atual e seguinte:

   `show bootvar`

Mostrar exemplo

```
(cs2) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

--------------------------------------------------------------------
 unit      active      backup     current-active        next-active
--------------------------------------------------------------------

    1     1.1.0.8     1.1.0.8            1.1.0.8            1.2.0.7
```

4. Instale o RCF compatível para a nova versão de imagem no interrutor.

   Se a versão RCF já estiver correta, abra as portas ISL.

   Mostrar exemplo

```
(cs2) #copy tftp://10.22.201.50//CN1610_CS_RCF_v1.2.txt nvram:script
CN1610_CS_RCF_v1.2.scr

Mode..................................... TFTP
Set Server IP.............................. 10.22.201.50
Path..................................... /
Filename.....................................
CN1610_CS_RCF_v1.2.txt
Data Type................................... Config Script
Destination Filename........................
CN1610_CS_RCF_v1.2.scr

File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.


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


Validating configuration script...
[the script is now displayed line by line]

Configuration script validated.
File transfer operation completed successfully.
```

   > A `.scr` extensão deve ser definida como parte do nome do arquivo antes de chamar o script. Esta extensão é para o sistema operacional FASTPATH.

   O switch valida o script automaticamente à medida que ele é baixado para o switch. A saída vai para o console.

5. Verifique se o script foi baixado e salvo no nome do arquivo que você deu.

Mostrar exemplo

```
(cs2) #script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
CN1610_CS_RCF_v1.2.scr                  2191

1 configuration script(s) found.
2541 Kbytes free.
```

6. Aplique o script ao switch.

Mostrar exemplo

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

7. Verifique se as alterações foram aplicadas ao switch e, em seguida, salve-as:

   `show running-config`

Mostrar exemplo

```
(cs2) #show running-config
```

8. Salve a configuração em execução para que ela se torne a configuração de inicialização quando você reiniciar o switch.

Mostrar exemplo

```
(cs2) #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!
```

9. Reinicie o switch.

Mostrar exemplo

```
(cs2) #reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

Passo 3: Valide a instalação

1. Faça login novamente e verifique se o switch está executando a nova versão do software FASTPATH.

Mostrar exemplo

```
(cs2) #show version

Switch: 1

System Description..............................  NetApp CN1610,
1.2.0.7,Linux
                                                   3.8.13-4ce360e8
Machine Type....................................  NetApp CN1610
Machine Model...................................  CN1610
Serial Number...................................  20211200106
Burned In MAC Address...........................  00:A0:98:21:83:69
Software Version................................  1.2.0.7
Operating System................................  Linux 3.8.13-
4ce360e8
Network Processing Device.......................  BCM56820_B0
Part Number.....................................  111-00893
CPLD version....................................  0x5


Additional Packages.............................  FASTPATH QOS
                                                   FASTPATH IPv6
Management
```

Após a conclusão da reinicialização, você deve fazer login para verificar a versão da imagem, exibir a configuração em execução e procurar a descrição na interface 3/64, que é o rótulo da versão para o RCF.

2. Abra as portas ISL no CS1, o interrutor ativo.

Mostrar exemplo

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

3. Verifique se os ISLs estão operacionais:

`show port-channel 3/1`

O campo Estado da ligação deve `Up` indicar .

Mostrar exemplo

```
(cs1) #show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  False
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

4. Abra a porta de cluster e0b em todos os nós:

   `network port modify`

   Você deve inserir os comandos nos consoles do controlador que possuem os respetivos LIFs de cluster.

   Mostrar exemplo

   O exemplo a seguir mostra a porta e0b sendo criada em node1 e node2:

   ```
   cluster1::*> network port modify -node node1 -port e0b -up-admin
   true
   cluster1::*> network port modify -node node2 -port e0b -up-admin
   true
   ```

5. Verifique se a porta e0b está ativa em todos os nós:

   `network port show -ipspace cluster`

Mostrar exemplo

```
cluster1::*> network port show -ipspace cluster

                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
node2
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
4 entries were displayed.
```

6. Verifique se o LIF está agora em (`true`casa) em ambos os nós:

   `network interface show -role cluster`

Mostrar exemplo

```
cluster1::*> network interface show -role cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.66.82/16   node1
e0a     true
            node1_clus2  up/up    169.254.206.128/16 node1
e0b     true
            node2_clus1  up/up    169.254.48.152/16  node2
e0a     true
            node2_clus2  up/up    169.254.42.74/16   node2
e0b     true
4 entries were displayed.
```

7. Mostrar o status dos membros do nó:

   `cluster show`

   Mostrar exemplo

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
2 entries were displayed.
```

8. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

9. Repita as etapas anteriores para instalar o software FASTPATH e o RCF no outro switch, CS1.

Configure o hardware para o switch NetApp CN1610

Para configurar o hardware e o software do switch para o ambiente do cluster, consulte o

"Guia de configuração e configuração do switch CN1601 e CN1610".

Migrar switches

Migre de um ambiente de cluster sem switch para um ambiente de cluster NetApp CN1610 comutado

Se você tiver um ambiente de cluster sem switch de dois nós existente, poderá migrar para um ambiente de cluster comutado de dois nós usando os switches de rede de cluster CN1610 que permitem que você escale além de dois nós.

Rever os requisitos

Antes de começar

Certifique-se de que tem o seguinte:

Para uma configuração sem switch de dois nós, certifique-se de que:

- A configuração sem switch de dois nós está corretamente configurada e funcionando.
- Os nós estão executando o ONTAP 8,2 ou posterior.
- Todas as portas do cluster estão `up` no estado.
- Todas as interfaces lógicas de cluster (LIFs) estão `up` no estado e em suas portas domésticas.

Para a configuração do interrutor do cluster CN1610:

- A infraestrutura de switch de cluster CN1610 está totalmente funcional em ambos os switches.
- Ambos os switches têm conetividade de rede de gerenciamento.
- Existe acesso à consola aos interrutores do cluster.
- As conexões de switch de nó para nó CN1610 e switch para switch usam cabos twinax ou de fibra.

  O"Hardware Universe" contém mais informações sobre cabeamento.

- Os cabos ISL (Inter-Switch Link) são conetados às portas 13 a 16 em ambos os switches CN1610.
- A personalização inicial de ambos os CN1610 switches está concluída.

  Qualquer personalização anterior do site, como SMTP, SNMP e SSH, deve ser copiada para os novos switches.

Informações relacionadas

- "Hardware Universe"
- "NetApp CN1601 e CN1610"
- "Configuração e instalação do switch CN1601 e CN1610"
- "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"

Migrar os switches

Sobre os exemplos

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos switches CN1610 são CS1 e CS2.
- Os nomes dos LIFs são clus1 e clus2.
- Os nomes dos nós são node1 e node2.
- O `cluster::*>` prompt indica o nome do cluster.
- As portas do cluster usadas neste procedimento são e1a e E2A.

  O"Hardware Universe" contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado (*>).

2. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   x é a duração da janela de manutenção em horas.

   > A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

   Mostrar exemplo

   O seguinte comando suprime a criação automática de casos por duas horas:

   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar portas

1. Desative todas as portas voltadas para o nó (não portas ISL) nos novos switches de cluster CS1 e CS2.

   Não deve desativar as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 12 voltadas para o nó estão desativadas no switch CS1:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

O exemplo a seguir mostra que as portas 1 a 12 voltadas para o nó estão desativadas no switch CS2:

```
(c2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

2. Verifique se o ISL e as portas físicas no ISL entre os dois switches CS1 e CS2 do cluster CN1610 são `up`:

   `show port-channel`

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão `up` no interrutor CS1:

```
(cs1)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

O exemplo a seguir mostra que as portas ISL estão `up` no interrutor CS2:

```
(cs2)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

3. Exibir a lista de dispositivos vizinhos:

   `show isdp neighbors`

   Este comando fornece informações sobre os dispositivos que estão conetados ao sistema.

Mostrar exemplo

O exemplo a seguir lista os dispositivos vizinhos no switch CS1:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
cs2                    0/13         11        S            CN1610
0/13
cs2                    0/14         11        S            CN1610
0/14
cs2                    0/15         11        S            CN1610
0/15
cs2                    0/16         11        S            CN1610
0/16
```

O exemplo a seguir lista os dispositivos vizinhos no switch CS2:

```
(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
cs1                    0/13         11        S            CN1610
0/13
cs1                    0/14         11        S            CN1610
0/14
cs1                    0/15         11        S            CN1610
0/15
cs1                    0/16         11        S            CN1610
0/16
```

4. Exibir a lista de portas do cluster:

```
network port show
```

Mostrar exemplo

O exemplo a seguir mostra as portas de cluster disponíveis:

```
cluster::*> network port show -ipspace Cluster
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0c       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0d       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0c       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0d       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4b       Cluster      Cluster          up   9000  auto/10000
healthy  false
12 entries were displayed.
```

5. Verifique se cada porta de cluster está conetada à porta correspondente em seu nó de cluster parceiro:

   `run * cdpd show-neighbors`

   Mostrar exemplo

   O exemplo a seguir mostra que as portas de cluster e1a e E2A estão conetadas à mesma porta em seu nó de parceiro de cluster:

```
cluster::*> run * cdpd show-neighbors
2 entries were acted on.

Node: node1
Local  Remote          Remote                 Remote           Hold
Remote
Port   Device          Interface              Platform         Time
Capability
------ --------------- ---------------------- ---------------- -----
----------
e1a    node2           e1a                    FAS3270           137
H
e2a    node2           e2a                    FAS3270           137
H


Node: node2

Local  Remote          Remote                 Remote           Hold
Remote
Port   Device          Interface              Platform         Time
Capability
------ --------------- ---------------------- ---------------- -----
----------
e1a    node1           e1a                    FAS3270           161
H
e2a    node1           e2a                    FAS3270           161
H
```

6. Verifique se todas as LIFs do cluster estão `up` operacionais e operacionais:

   `network interface show -vserver Cluster`

   Cada LIF de cluster deve ser exibido `true` na coluna "is Home".

Mostrar exemplo

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up      10.10.10.1/16 node1         e1a
true
            clus2      up/up      10.10.10.2/16 node1         e2a
true
node2
            clus1      up/up      10.10.11.1/16 node2         e1a
true
            clus2      up/up      10.10.11.2/16 node2         e2a
true

4 entries were displayed.
```

Os seguintes comandos de modificação e migração nas etapas 10 a 13 devem ser feitos a partir do nó local.

7. Verifique se todas as portas do cluster são `up`:

   `network port show -ipspace Cluster`

Mostrar exemplo

```
cluster::*> network port show -ipspace Cluster

                                         Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link  MTU   Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ----- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

8. Defina o `-auto-revert` parâmetro como `false` no cluster LIFs clus1 e clus2 em ambos os nós:

   `network interface modify`

   Mostrar exemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

   Para a versão 8,3 e posterior, use o seguinte comando: `network interface modify -vserver Cluster -lif * -auto-revert false`

9. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. migre clus1 para a porta E2A no console de cada nó:

   `network interface migrate`

   Mostrar exemplo

   O exemplo a seguir mostra o processo de migração do clus1 para a porta E2A em node1 e node2:

   ```
   cluster::*> network interface migrate -vserver node1 -lif clus1
   -source-node node1 -dest-node node1 -dest-port e2a
   cluster::*> network interface migrate -vserver node2 -lif clus1
   -source-node node2 -dest-node node2 -dest-port e2a
   ```

   Para a versão 8,3 e posterior, use o seguinte comando: `network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination -port e2a`

2. Verifique se a migração ocorreu:

```
network interface show -vserver Cluster
```

Mostrar exemplo

O exemplo a seguir verifica se o clus1 foi migrado para a porta E2A em node1 e node2:

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e2a
false
            clus2      up/up    10.10.10.2/16   node1         e2a
true
node2
            clus1      up/up    10.10.11.1/16   node2         e2a
false
            clus2      up/up    10.10.11.2/16   node2         e2a
true

4 entries were displayed.
```

3. Encerre a porta e1a do cluster em ambos os nós:

```
network port modify
```

Mostrar exemplo

O exemplo a seguir mostra como desligar a porta e1a em node1 e node2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin
false
cluster::*> network port modify -node node2 -port e1a -up-admin
false
```

4. Verifique o status da porta:

```
network port show
```

Mostrar exemplo

O exemplo a seguir mostra que a porta e1a está `down` em node1 e node2:

```
cluster::*> network port show -role cluster
                                        Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        down  9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        down  9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

5. Desconete o cabo da porta de cluster e1a no node1 e conete o e1a à porta 1 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches CN1610.

   O "Hardware Universe" contém mais informações sobre cabeamento.

6. Desconete o cabo da porta de cluster e1a no node2 e conete o e1a à porta 2 no switch de cluster CS1, usando o cabeamento apropriado suportado pelos switches CN1610.
7. Habilite todas as portas voltadas para o nó no switch de cluster CS1.

   Mostrar exemplo

   O exemplo a seguir mostra que as portas 1 a 12 estão ativadas no switch CS1:

   ```
   (cs1)# configure
   (cs1)(Config)# interface 0/1-0/12
   (cs1)(Interface 0/1-0/12)# no shutdown
   (cs1)(Interface 0/1-0/12)# exit
   (cs1)(Config)# exit
   ```

8. Ative a primeira porta de cluster e1a em cada nó:

`network port modify`

Mostrar exemplo

O exemplo a seguir mostra como ativar a porta e1a em node1 e node2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin true
cluster::*> network port modify -node node2 -port e1a -up-admin true
```

9. Verifique se todas as portas do cluster são `up`:

`network port show -ipspace Cluster`

Mostrar exemplo

O exemplo a seguir mostra que todas as portas de cluster estão `up` em node1 e node2:

```
cluster::*> network port show -ipspace Cluster
                                     Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

10. Reverter clus1 (que foi migrado anteriormente) para e1a em ambos os nós:

`network interface revert`

Mostrar exemplo

O exemplo a seguir mostra como reverter clus1 para a porta e1a em node1 e node2:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```

Para a versão 8,3 e posterior, use o seguinte comando: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

11. Verifique se todas as LIFs do cluster são `up`, operacionais e exibidas como `true` na coluna "está Home":

`network interface show -vserver Cluster`

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão `up` em node1 e node2 e que os resultados da coluna "está em Casa" são `true`:

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e1a
true
            clus2      up/up    10.10.10.2/16   node1         e2a
true
node2
            clus1      up/up    10.10.11.1/16   node2         e1a
true
            clus2      up/up    10.10.11.2/16   node2         e2a
true

4 entries were displayed.
```

12. Exibir informações sobre o status dos nós no cluster:

`cluster show`

Mostrar exemplo

O exemplo a seguir exibe informações sobre a integridade e a elegibilidade dos nós no cluster:

```
cluster::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          false
node2                 true    true          false
```

13. Migre clus2 para a porta e1a no console de cada nó:

`network interface migrate`

Mostrar exemplo

O exemplo a seguir mostra o processo de migração do clus2 para a porta e1a em node1 e node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2
-source-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2
-source-node node2 -dest-node node2 -dest-port e1a
```

Para a versão 8,3 e posterior, use o seguinte comando: `network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a`

14. Verifique se a migração ocorreu:

`network interface show -vserver Cluster`

Mostrar exemplo

O exemplo a seguir verifica se o clus2 foi migrado para a porta e1a em node1 e node2:

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e1a
true
            clus2      up/up    10.10.10.2/16   node1         e1a
false
node2
            clus1      up/up    10.10.11.1/16   node2         e1a
true
            clus2      up/up    10.10.11.2/16   node2         e1a
false

4 entries were displayed.
```

15. Encerre a porta E2A do cluster em ambos os nós:

`network port modify`

Mostrar exemplo

O exemplo a seguir mostra como desligar a porta E2A em node1 e node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

16. Verifique o status da porta:

`network port show`

Mostrar exemplo

O exemplo a seguir mostra que a porta E2A está `down` em node1 e node2:

```
cluster::*> network port show -role cluster
                                     Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        down  9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        down  9000  true/true  full/full
auto/10000

4 entries were displayed.
```

17. Desconete o cabo da porta de cluster E2A no node1 e conete o E2A à porta 1 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches CN1610.
18. Desconete o cabo da porta de cluster E2A no node2 e conete o E2A à porta 2 no switch de cluster CS2, usando o cabeamento apropriado suportado pelos switches CN1610.
19. Habilite todas as portas voltadas para o nó no switch de cluster CS2.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1 a 12 estão ativadas no switch CS2:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# no shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

20. Ative a segunda porta de cluster E2A em cada nó.

Mostrar exemplo

O exemplo a seguir mostra como ativar a porta E2A em node1 e node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

21. Verifique se todas as portas do cluster são `up`:

`network port show -ipspace Cluster`

Mostrar exemplo

O exemplo a seguir mostra que todas as portas de cluster estão `up` em node1 e node2:

```
cluster::*> network port show -ipspace Cluster
                                     Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

22. Reverter clus2 (que foi migrado anteriormente) para E2A em ambos os nós:

`network interface revert`

Mostrar exemplo

O exemplo a seguir mostra como reverter clus2 para a porta E2A em node1 e node2:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

Para a versão 8,3 e posterior, os comandos são:
`cluster::*> network interface revert -vserver Cluster -lif node1_clus2` E.
`cluster::*> network interface revert -vserver Cluster -lif node2_clus2`

Passo 3: Conclua a configuração

1. Verifique se todas as interfaces são exibidas `true` na coluna "está Home":

   `network interface show -vserver Cluster`

Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs estão `up` em node1 e node2 e que os resultados da coluna "está em Casa" são `true`:

```
cluster::*> network interface show -vserver Cluster

             Logical    Status     Network            Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask       Node
Port    Home
-----------  ---------- ---------- ------------------ -----------
------- ----
node1
             clus1      up/up      10.10.10.1/16      node1
e1a     true
             clus2      up/up      10.10.10.2/16      node1
e2a     true
node2
             clus1      up/up      10.10.11.1/16      node2
e1a     true
             clus2      up/up      10.10.11.2/16      node2
e2a     true
```

2. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se ambos os nós têm duas conexões para cada switch:

```
show isdp neighbors
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambos os switches:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
node1                  0/1          132       H            FAS3270
e1a
node2                  0/2          163       H            FAS3270
e1a
cs2                    0/13         11        S            CN1610
0/13
cs2                    0/14         11        S            CN1610
0/14
cs2                    0/15         11        S            CN1610
0/15
cs2                    0/16         11        S            CN1610
0/16

(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
node1                  0/1          132       H            FAS3270
e2a
node2                  0/2          163       H            FAS3270
e2a
cs1                    0/13         11        S            CN1610
0/13
cs1                    0/14         11        S            CN1610
0/14
cs1                    0/15         11        S            CN1610
0/15
cs1                    0/16         11        S            CN1610
0/16
```

2. Exiba informações sobre os dispositivos em sua configuração:

   `network device discovery show`

3. Desative as configurações sem switch de dois nós em ambos os nós usando o comando de privilégio avançado:

   `network options detect-switchless modify`

   Mostrar exemplo

   O exemplo a seguir mostra como desativar as configurações sem switch:

   ```
   cluster::*> network options detect-switchless modify -enabled false
   ```

   Para a versão 9,2 e posterior, ignore esta etapa, pois a configuração é convertida automaticamente.

4. Verifique se as definições estão desativadas:

   `network options detect-switchless-cluster show`

   Mostrar exemplo

   A `false` saída no exemplo a seguir mostra que as configurações estão desativadas:

   ```
   cluster::*> network options detect-switchless-cluster show
   Enable Switchless Cluster Detection: false
   ```

   Para a versão 9,2 e posterior, aguarde até `Enable Switchless Cluster` que seja definido como false. Isso pode levar até três minutos.

5. Configure os clusters clus1 e clus2 para reverter automaticamente em cada nó e confirmar.

Mostrar exemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```

Para a versão 8,3 e posterior, use o seguinte comando: `network interface modify -vserver Cluster -lif * -auto-revert true` Para habilitar a reversão automática em todos os nós do cluster.

6. Verifique o status dos membros do nó no cluster:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra informações sobre a integridade e a elegibilidade dos nós no cluster:

   ```
   cluster::*> cluster show
   Node                 Health  Eligibility   Epsilon
   -------------------- ------- ------------  ------------
   node1                true    true          false
   node2                true    true          false
   ```

7. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   `system node autosupport invoke -node * -type all -message MAINT=END`

   Mostrar exemplo

   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

8. Altere o nível de privilégio de volta para admin:

   `set -privilege admin`

Substitua os interrutores

Substitua um interrutor do cluster do NetApp CN1610

Siga estas etapas para substituir um switch NetApp CN1610 defeituoso em uma rede de cluster. Este é um procedimento sem interrupções (NDU).

Rever os requisitos

Antes de começar

Antes de realizar a substituição do switch, as condições a seguir devem existir antes de executar a substituição do switch no ambiente atual e no switch de substituição para o cluster existente e a infraestrutura de rede:

- O cluster existente deve ser verificado como completamente funcional, com pelo menos um switch de cluster totalmente conetado.
- Todas as portas do cluster devem ser **up**.
- Todas as interfaces lógicas de cluster (LIFs) devem estar ativas e não devem ter sido migradas.
- O comando ONTAP cluster `ping-cluster -node node1` deve indicar que a conetividade básica e a comunicação maior do que a PMTU são bem-sucedidas em todos os caminhos.

Ativar o registo da consola

O NetApp recomenda fortemente que você ative o log do console nos dispositivos que você está usando e execute as seguintes ações ao substituir o switch:

- Deixe o AutoSupport ativado durante a manutenção.
- Acione um AutoSupport de manutenção antes e depois da manutenção para desativar a criação de casos durante a manutenção. Consulte este artigo da base de dados de Conhecimento "SU92: Como suprimir a criação automática de casos durante as janelas de manutenção programada" para obter mais detalhes.
- Ativar o registo de sessão para quaisquer sessões CLI. Para obter instruções sobre como ativar o registo de sessão, consulte a secção "saída de sessão de registo" neste artigo da base de dados de conhecimento "Como configurar o PuTTY para uma conetividade ideal aos sistemas ONTAP" .

Substitua o interrutor

Sobre esta tarefa

Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.

Os exemplos deste procedimento utilizam a seguinte nomenclatura de nó e switch de cluster:

- Os nomes dos dois switches de cluster CN1610 são `cs1` e `cs2`.
- O nome do interrutor CN1610 que deve ser substituído (o interrutor com defeito) é `old_cs1`.
- O nome do novo interrutor CN1610 (o interrutor de substituição) é `new_cs1`.
- O nome do switch parceiro que não está sendo substituído é `cs2`.

Passos

1. Confirme se o arquivo de configuração de inicialização corresponde ao arquivo de configuração em execução. Você deve salvar esses arquivos localmente para uso durante a substituição.

Os comandos de configuração no exemplo a seguir são para FASTPATH 1,2.0,7:

Mostrar exemplo

```
(old_cs1)> enable
(old_cs1)# show running-config
(old_cs1)# show startup-config
```

2. Crie uma cópia do arquivo de configuração em execução.

   O comando no exemplo a seguir é para FASTPATH 1,2.0,7:

   Mostrar exemplo

```
(old_cs1)# show running-config filename.scr
Config script created successfully.
```

Você pode usar qualquer nome de arquivo, exceto `CN1610_CS_RCF_v1.2.scr`. O nome do ficheiro tem de ter a extensão **.scr**.

1. Salve o arquivo de configuração em execução do switch para um host externo em preparação para a substituição.

   Mostrar exemplo

```
(old_cs1)# copy nvram:script filename.scr
scp://<Username>@<remote_IP_address>/path_to_file/filename.scr
```

2. Verifique se as versões switch e ONTAP correspondem à matriz de compatibilidade. Consulte a "Switches NetApp CN1601 e CN1610" página para obter detalhes.
3. No "Página de transferências de software" site de suporte da NetApp, selecione switches de cluster NetApp para baixar as versões apropriadas de RCF e FASTPATH.
4. Configure um servidor TFTP (Trivial File Transfer Protocol) com o FASTPATH, RCF e o arquivo de configuração salvo `.scr` para uso com o novo switch.
5. Conete a porta serial (o conetor RJ-45 rotulado "IOIOI" no lado direito do switch) a um host disponível com emulação de terminal.
6. No host, defina as configurações de conexão do terminal serial:
   a. 9600 baud
   b. 8 bits de dados
   c. 1 bit de paragem

d. paridade: nenhuma

e. controle de fluxo: nenhum

7. Conete a porta de gerenciamento (a porta chave RJ-45 no lado esquerdo do switch) à mesma rede onde o servidor TFTP está localizado.

8. Prepare-se para se conetar à rede com o servidor TFTP.

   Se estiver a utilizar o DHCP (Dynamic Host Configuration Protocol), não terá de configurar um endereço IP para a central neste momento. A porta de serviço está definida para utilizar DHCP por predefinição. A porta de gerenciamento de rede está definida como nenhuma para as configurações de protocolo IPv4 e IPv6. Se a porta Wrench estiver conetada a uma rede que tenha um servidor DHCP, as configurações do servidor serão configuradas automaticamente.

   Para definir um endereço IP estático, você deve usar o protocolo de serviceport, o protocolo de rede e os comandos ip de serviceport.

   Mostrar exemplo

   ```
   (new_cs1)# serviceport ip <ipaddr> <netmask> <gateway>
   ```

9. Opcionalmente, se o servidor TFTP estiver em um laptop, conete o switch CN1610 ao laptop usando um cabo Ethernet padrão e configure sua porta de rede na mesma rede com um endereço IP alternativo.

   Você pode usar o `ping` comando para verificar o endereço. Se você não conseguir estabelecer a conetividade, use uma rede não roteada e configure a porta de serviço usando IP 192,168.x ou 172,16.x. Você pode reconfigurar a porta de serviço para o endereço IP de gerenciamento de produção em uma data posterior.

10. Opcionalmente, verifique e instale as versões apropriadas do software RCF e FASTPATH para o novo switch. Se você verificou que o novo switch está corretamente configurado e não requer atualizações para o software RCF e FASTPATH, você deve ir para a etapa 13.

    a. Verifique as novas definições do interrutor.

       Mostrar exemplo

       ```
       (new_cs1)> enable
       (new_cs1)# show version
       ```

    b. Transfira o RCF para o novo interrutor.

Mostrar exemplo

```
(new_cs1)# copy tftp://<server_ip_address>/CN1610_CS_RCF_v1.2.txt
nvram:script CN1610_CS_RCF_v1.2.scr
Mode.   TFTP
Set Server IP.  172.22.201.50
Path.   /
Filename.....................................
CN1610_CS_RCF_v1.2.txt
Data Type..................................... Config Script
Destination Filename.........................
CN1610_CS_RCF_v1.2.scr
File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

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...
Validating configuration script...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script validated.
File transfer operation completed successfully.
```

c. Verifique se o RCF foi transferido para o comutador.

Mostrar exemplo

```
(new_cs1)# script list
Configuration Script Nam   Size(Bytes)
-------------------------- -----------
CN1610_CS_RCF_v1.1.scr            2191
CN1610_CS_RCF_v1.2.scr            2240
latest_config.scr                 2356

4 configuration script(s) found.
2039 Kbytes free.
```

11. Aplique o RCF no interrutor CN1610.

Mostrar exemplo

```
(new_cs1)# script apply CN1610_CS_RCF_v1.2.scr
Are you sure you want to apply the configuration script? (y/n) y
...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script 'CN1610_CS_RCF_v1.2.scr' applied. Note that the
script output will go to the console.
After the script is applied, those settings will be active in the
running-config file. To save them to the startup-config file, you
must use the write memory command, or if you used the reload answer
yes when asked if you want to save the changes.
```

a. Salve o arquivo de configuração em execução para que ele se torne o arquivo de configuração de inicialização quando você reiniciar o switch.

Mostrar exemplo

```
(new_cs1)# 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!
```

b. Transfira a imagem para o interrutor CN1610.

Mostrar exemplo

```
(new_cs1)# copy
tftp://<server_ip_address>/NetApp_CN1610_1.2.0.7.stk active
Mode.   TFTP
Set Server IP.  tftp_server_ip_address
Path.   /
Filename.....................................
NetApp_CN1610_1.2.0.7.stk
Data Type.  Code
Destination Filename.   active

Management access will be blocked for the duration of the
transfer

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

TFTP Code transfer starting...

File transfer operation completed successfully.
```

c. Execute a nova imagem de inicialização ativa reiniciando o switch.

   O switch deve ser reinicializado para o comando no passo 6 para refletir a nova imagem. Há duas visualizações possíveis para uma resposta que você pode ver depois de digitar o comando reload.

Mostrar exemplo

```
(new_cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved! System will now restart!
.
.
.
Cluster Interconnect Infrastructure

User:admin Password: (new_cs1) >*enable*
```

a. Copie o arquivo de configuração salvo do switch antigo para o novo switch.

Mostrar exemplo

```
(new_cs1)# copy tftp://<server_ip_address>/<filename>.scr
nvram:script <filename>.scr
```

b. Aplique a configuração guardada anteriormente ao novo interrutor.

Mostrar exemplo

```
(new_cs1)# script apply <filename>.scr
Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

c. Salve o arquivo de configuração em execução no arquivo de configuração de inicialização.

Mostrar exemplo

```
(new_cs1)# write memory
```

12. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:
`system node autosupport invoke -node * -type all - message MAINT=xh`

    x é a duração da janela de manutenção em horas.

    A mensagem AutoSupport notifica o suporte técnico desta tarefa de manutenção para que a criação automática de casos seja suprimida durante a janela de manutenção.

13. No novo switch new_CS1, faça login como usuário admin e encerre todas as portas que estão conetadas às interfaces do cluster de nós (portas 1 a 12).

Mostrar exemplo

```
User:*admin*
Password:
(new_cs1)> enable
(new_cs1)#
(new_cs1)# config
(new_cs1)(config)# interface 0/1-0/12
(new_cs1)(interface 0/1-0/12)# shutdown
(new_cs1)(interface 0/1-0/12)# exit
(new_cs1)# write memory
```

14. Migre as LIFs de cluster das portas que estão conetadas ao switch Old_CS1.

    É necessário migrar cada LIF de cluster a partir da interface de gerenciamento do nó atual.

    Mostrar exemplo

    ```
    cluster::> set -privilege advanced
    cluster::> network interface migrate -vserver <vserver_name> -lif
    <Cluster_LIF_to_be_moved> - sourcenode <current_node> -dest-node
    <current_node> -dest-port <cluster_port_that_is_UP>
    ```

15. Verifique se todas as LIFs de cluster foram movidas para a porta de cluster apropriada em cada nó.

    Mostrar exemplo

    ```
    cluster::> network interface show -role cluster
    ```

16. Encerre as portas do cluster que estão conetadas ao switch que você substituiu.

    Mostrar exemplo

    ```
    cluster::*> network port modify -node <node_name> -port
    <port_to_admin_down> -up-admin false
    ```

17. Verifique a integridade do cluster.

Mostrar exemplo

```
cluster::*> cluster show
```

18. Verifique se as portas estão inativas.

Mostrar exemplo

```
cluster::*> cluster ping-cluster -node <node_name>
```

19. No interrutor CS2, desligue as portas ISL 13 a 16.

Mostrar exemplo

```
(cs2)# config
(cs2)(config)# interface 0/13-0/16
(cs2)(interface 0/13-0/16)# shutdown
(cs2)# show port-channel 3/1
```

20. Verifique se o administrador de armazenamento está pronto para a substituição do switch.
21. Remova todos os cabos do switch old_CS1 e conete os cabos às mesmas portas do switch new_CS1.
22. No switch CS2, abra as portas ISL 13 a 16.

Mostrar exemplo

```
(cs2)# config
(cs2)(config)# interface 0/13-0/16
(cs2)(interface 0/13-0/16)# no shutdown
```

23. Abra as portas no novo switch que estão associadas aos nós de cluster.

Mostrar exemplo

```
(new_cs1)# config
(new_cs1)(config)# interface 0/1-0/12
(new_cs1)(interface 0/13-0/16)# no shutdown
```

24. Em um único nó, abra a porta do nó do cluster que está conetada ao switch substituído e confirme se o link está ativo.

Mostrar exemplo

```
cluster::*> network port modify -node node1 -port
<port_to_be_onlined> -up-admin true
cluster::*> network port show -role cluster
```

25. Reverta as LIFs de cluster associadas à porta na etapa 25 no mesmo nó.

Neste exemplo, os LIFs no node1 são revertidos com sucesso se a coluna "está em Casa" for verdadeira.

Mostrar exemplo

```
cluster::*> network interface revert -vserver node1 -lif
<cluster_lif_to_be_reverted>
cluster::*> network interface show -role cluster
```

26. Se o LIF do cluster do primeiro nó estiver ativo e for revertido para sua porta inicial, repita as etapas 25 e 26 para abrir as portas do cluster e reverter as LIFs do cluster nos outros nós do cluster.
27. Exibir informações sobre os nós no cluster.

Mostrar exemplo

```
cluster::*> cluster show
```

28. Confirme se o arquivo de configuração de inicialização e o arquivo de configuração em execução estão corretos no switch substituído. Este arquivo de configuração deve corresponder à saída no passo 1.

Mostrar exemplo

```
(new_cs1)> enable
(new_cs1)# show running-config
(new_cs1)# show startup-config
```

29. Se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Substitua os switches de cluster NetApp CN1610 por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para um em que dois nós estejam diretamente conetados para o ONTAP 9.3 e posterior.

Rever os requisitos

Diretrizes

Reveja as seguintes diretrizes:

- Migrar para uma configuração de cluster sem switch de dois nós é uma operação sem interrupções. A maioria dos sistemas tem duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar esse procedimento para sistemas com um número maior de portas de interconexão de cluster dedicadas em cada nó, como quatro, seis ou oito.
- Não é possível usar o recurso de interconexão de cluster sem switch com mais de dois nós.
- Se você tiver um cluster de dois nós existente que usa switches de interconexão de cluster e estiver executando o ONTAP 9.3 ou posterior, poderá substituir os switches por conexões diretas e de retorno entre os nós.

Antes de começar

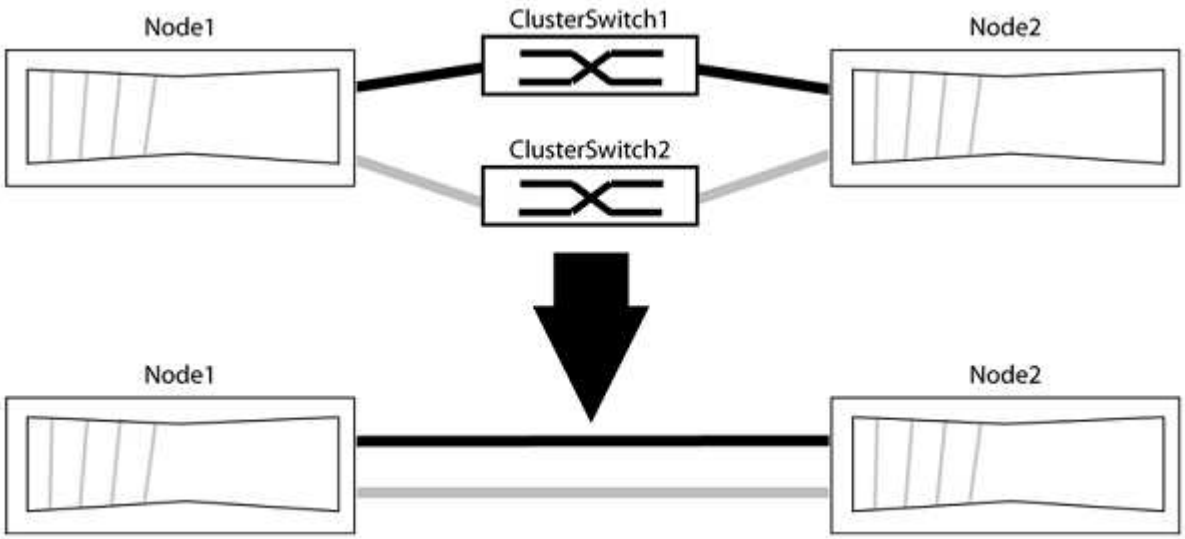
Certifique-se de que tem o seguinte:

- Um cluster íntegro que consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP.
- Cada nó com o número necessário de portas de cluster dedicadas, que fornecem conexões redundantes de interconexão de cluster para oferecer suporte à configuração do sistema. Por exemplo, há duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migrar os switches

Sobre esta tarefa

O procedimento a seguir remove os switches de cluster em um cluster de dois nós e substitui cada conexão com o switch por uma conexão direta com o nó do parceiro.



Sobre os exemplos

Os exemplos no procedimento a seguir mostram nós que estão usando "e0a" e "e0b" como portas de cluster. Seus nós podem estar usando portas de cluster diferentes, pois variam de acordo com o sistema.

Passo 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   É apresentado o aviso avançado `*>`.

2. O ONTAP 9.3 e versões posteriores são compatíveis com a detecção automática de clusters sem switch, que é habilitada por padrão.

   Você pode verificar se a deteção de clusters sem switch está ativada executando o comando de privilégio avançado:

   ```
   network options detect-switchless-cluster show
   ```

   Mostrar exemplo

   A saída de exemplo a seguir mostra se a opção está ativada.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Ativar deteção de cluster sem switch" for `false`, entre em Contato com o suporte da NetApp.

3. Se o AutoSupport estiver ativado neste cluster, suprimir a criação automática de casos invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message
   MAINT=<number_of_hours>h
   ```

   ```
   `h`onde está a duração da janela de manutenção em horas. A mensagem
   notifica o suporte técnico desta tarefa de manutenção para que possa
   suprimir a criação automática de casos durante a janela de manutenção.
   ```

   No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

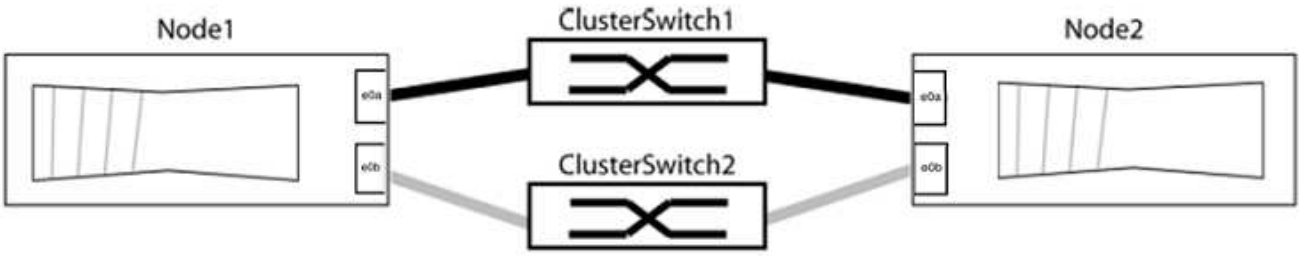
   Mostrar exemplo

   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Etapa 2: Configurar portas e cabeamento

1. Organize as portas do cluster em cada switch em grupos para que as portas do cluster em group1 passem para o cluster switch1 e as portas do cluster em group2 passem para o cluster switch2. Estes grupos são necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade do xref:./switch-netapp-cn1610/+ `network port show -ipspace Cluster`

   No exemplo a seguir para nós com portas de cluster "e0a" e "e0b", um grupo é identificado como "node1:e0a" e "node2:e0a" e o outro grupo como "node1:e0b" e "node2:e0b". Seus nós podem estar usando portas de cluster diferentes porque variam de acordo com o sistema.



   Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Status de integridade".

Mostrar exemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Confirme se todas as LIFs de cluster estão em suas portas residenciais.

   Verifique se a coluna "is-home" é `true` para cada um dos LIFs de cluster:

   `network interface show -vserver Cluster -fields is-home`

Mostrar exemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se houver LIFs de cluster que não estão em suas portas residenciais, reverta esses LIFs para suas portas residenciais:

```
network interface revert -vserver Cluster -lif *
```

4. Desativar a reversão automática para as LIFs do cluster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Verifique se todas as portas listadas na etapa anterior estão conetadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna "dispositivo descoberto" deve ser o nome do switch de cluster ao qual a porta está conetada.

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conetadas aos switches do cluster "CS1" e "CS2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Verifique se o cluster está saudável:

   ```
   cluster ring show
   ```

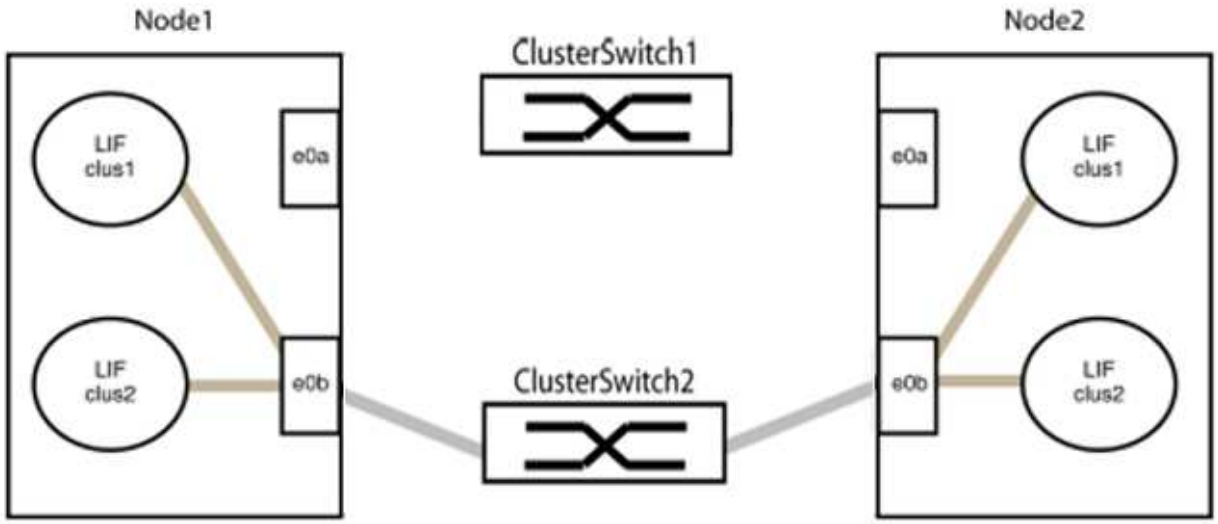
   Todas as unidades devem ser principais ou secundárias.

2. Configure a configuração sem switch para as portas do grupo 1.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group1 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

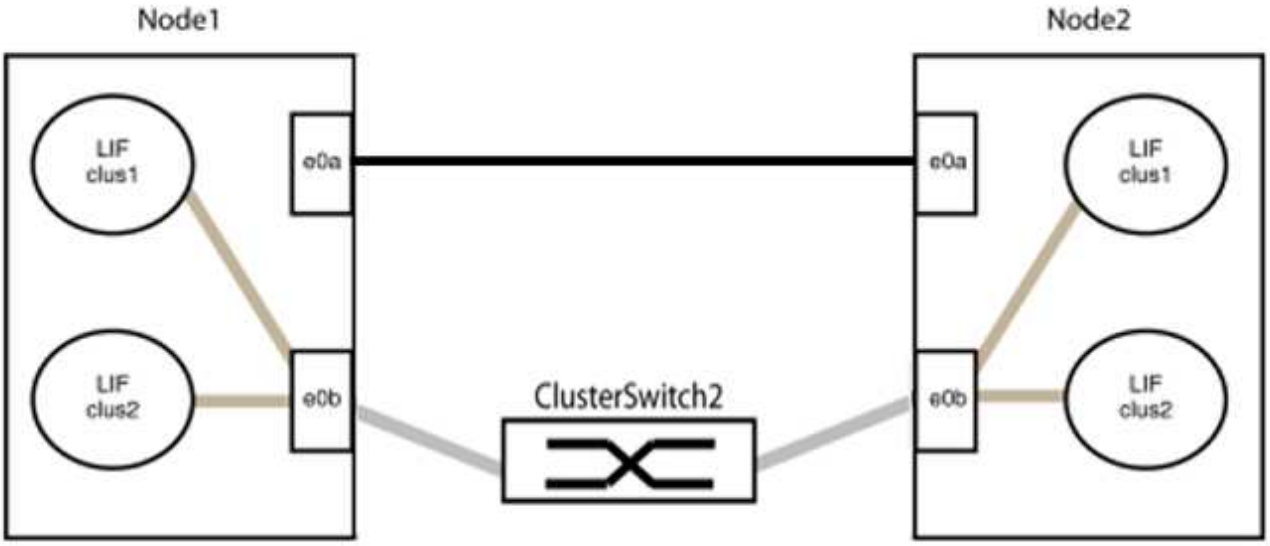
   a. Desconete todos os cabos das portas do group1 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0a" em cada nó e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Faça o cabo das portas em group1 de volta para trás.

No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2:



3. A opção de rede de cluster sem switch faz a transição de `false` para `true`. Isso pode levar até 45 segundos. Confirme se a opção sem switch está definida como `true`:

`network options switchless-cluster show`

O exemplo a seguir mostra que o cluster sem switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

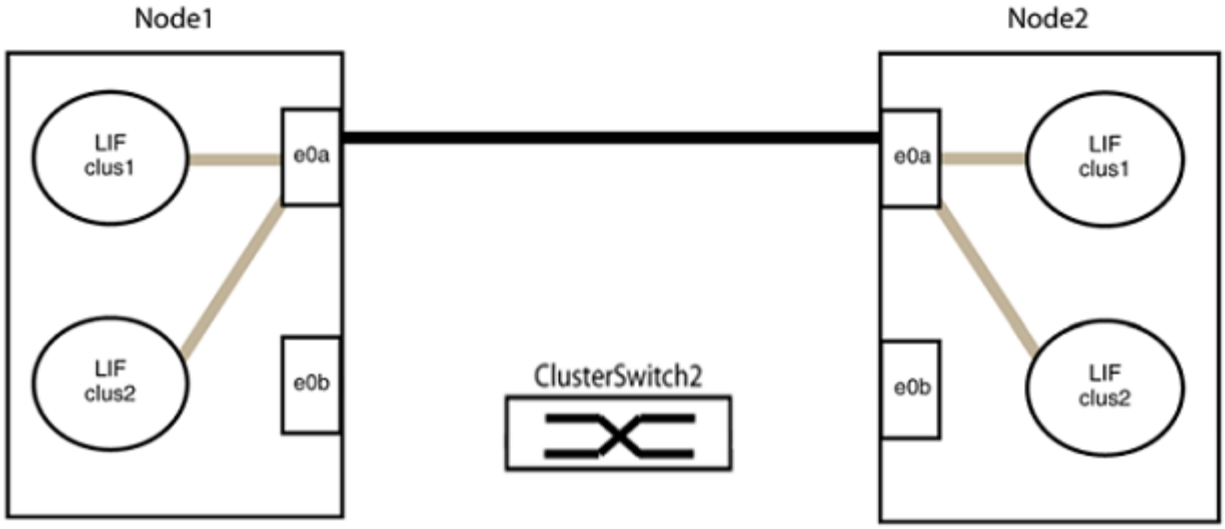
Antes de prosseguir para a próxima etapa, você deve esperar pelo menos dois minutos para confirmar uma conexão de trabalho de volta para trás no grupo 1.

1. Configure a configuração sem switch para as portas no grupo 2.

   Para evitar possíveis problemas de rede, você deve desconetar as portas do group2 e reconectá-las o mais rápido possível, por exemplo, **em menos de 20 segundos**.

   a. Desconete todos os cabos das portas do group2 ao mesmo tempo.

      No exemplo a seguir, os cabos são desconetados da porta "e0b" em cada nó e o tráfego de cluster continua através da conexão direta entre as portas "e0a":



b. Faça o cabo das portas em group2 de volta para trás.

   No exemplo seguinte, "e0a" no node1 está ligado a "e0a" no node2 e "e0b" no node1 está ligado a "e0b" no node2:

Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conetadas:

   `network device-discovery show -port cluster_port`

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conetadas à porta correspondente no parceiro de cluster:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Reative a reversão automática para as LIFs do cluster:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Verifique se todos os LIFs estão em casa. Isso pode levar alguns segundos.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostrar exemplo

Os LIFs foram revertidos se a coluna "está em Casa" for `true`, como mostrado para `node1_clus2` e `node2_clus2` no exemplo a seguir:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Se qualquer LIFS de cluster não retornou às portas iniciais, reverta-as manualmente do nó local:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Verifique o status do cluster dos nós a partir do console do sistema de qualquer nó:

   `cluster show`

   Mostrar exemplo

   O exemplo a seguir mostra epsilon em ambos os nós a ser `false`:

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Verifique a conectividade das interfaces de cluster remotas:

ONTAP 9.9,1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conetividade de cluster e, em seguida, exibir os detalhes:

`network interface check cluster-connectivity start` e `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: espere alguns segundos antes de executar o `show` comando para exibir os detalhes.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos os lançamentos do ONTAP

Para todas as versões do ONTAP, você também pode usar o `cluster ping-cluster -node <name>` comando para verificar a conetividade:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. se você suprimiu a criação automática de casos, reative-a invocando uma mensagem AutoSupport:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Para obter mais informações, "NetApp KB artigo 1010449: Como suprimir a criação automática de casos durante janelas de manutenção programada"consulte .

2. Altere o nível de privilégio de volta para admin:

   ```
   set -privilege admin
   ```

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE 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.