



Documentação de switches para sistemas de armazenamento ONTAP

Install and maintain

NetApp
March 27, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-systems-switches/index.html> on March 27, 2026. Always check docs.netapp.com for the latest.

Índice

Documentação de switches para sistemas de armazenamento ONTAP	1
Começar	2
O que há de novo para switches?	2
Novo suporte para interruptor	2
Saiba mais sobre sistemas AFX, cluster, armazenamento e switches compartilhados	3
Interruptores de sistemas AFX	3
Comutadores de cluster	4
Interruptores de armazenamento	4
Switches compartilhados	4
Interruptores de fim de disponibilidade	4
Comece a usar os sistemas AFX, cluster, armazenamento e switches compartilhados	4
Interruptores de sistemas AFX	8
Cisco Nexus 9332D-GX2B	8
Começar	8
Instalar hardware	11
Configurar software	11
Redefinir o switch 9332D-GX2B para os padrões de fábrica	121
Substituir um switch Cisco Nexus 9332D-GX2B	121
Cisco Nexus 9364D-GX2A	149
Começar	149
Instalar hardware	152
Configurar software	153
Redefinir o switch 9364D-GX2A para os padrões de fábrica	280
Substituir um switch Cisco Nexus 9364D-GX2A	280
Comutadores de cluster	309
BES-53248 com suporte da Broadcom	309
Começar	309
Instale o hardware	313
Configurar o software	316
Redefinir o switch do cluster BES-53248 para os padrões de fábrica	413
Atualize o switch	414
Migre os switches	458
Substitua os interruptores	496
Cisco Nexus 9336C-FX2 ou 9336C-FX2-T	524
Começar	524
Instale o hardware	530
Configurar o software	541
Redefinir os switches do cluster 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica	613
Migre os switches	613
Substitua os interruptores	668
NVIDIA SN2100	700
Começar	700
Instale o hardware	703

Configurar o software	713
Redefinir o switch do cluster SN2100 para os padrões de fábrica	789
Migre os switches	791
Substitua os interruptores	848
Interruptores de armazenamento	883
Cisco Nexus 9336C-FX2 ou 9336C-FX2-T	883
Começar	883
Instale o hardware	887
Configurar o software	899
Redefinir os switches de armazenamento 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica ..	943
Substituir switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T	943
Cisco Nexus 3232C	949
Começar	949
Instalar hardware	953
Configurar software	959
Redefina o switch de armazenamento 3232C para os padrões de fábrica	992
Substitua um switch de armazenamento Cisco Nexus 3232C	992
Atualizar um switch de armazenamento Cisco Nexus 3232C	999
NVIDIA SN2100	1014
Começar	1014
Instalar hardware	1016
Configurar software	1026
Redefinir o switch de armazenamento SN2100 para os padrões de fábrica	1056
Migrar switches	1058
Substitua um switch de armazenamento NVIDIA SN2100	1068
Switches compartilhados	1076
Cisco Nexus 9336C-FX2	1076
Começar	1076
Instale o hardware	1078
Configurar o software	1089
Redefinir o switch compartilhado 9336C-FX2 para os padrões de fábrica	1168
Migrar switches	1169
Substitua um switch compartilhado Cisco Nexus 9336C-FX2	1208
Monitorar o estado do interruptor	1227
Visão geral do monitor de integridade do switch	1227
Configure o monitoramento de integridade do switch	1227
Visão geral da configuração	1227
Configurar coleta de logs	1227
Configure o SNMPv3 para o seu switch (Opcional)	1234
Verifique o estado do interruptor	1252
Visão geral do check-up de saúde	1252
Gerenciar o monitoramento de switches Ethernet	1252
Verifique o monitoramento dos switches Ethernet	1254
Solucionar problemas de alertas	1255
Coleta de registros	1255

Visão geral da coleta de logs	1255
Solução de problemas na coleta de logs	1255
Interruptores de fim de disponibilidade	1257
Interruptores de fim de disponibilidade	1257
Anúncios de fim de vendas e fim de vida útil	1257
Cisco Nexus 3232C	1257
Começar	1257
Instalar hardware	1261
Configurar software	1270
Redefinir o switch do cluster 3232C para os padrões de fábrica	1333
Migrar switches	1333
Substitua os interruptores	1355
Cisco Nexus 3132Q-V	1397
Começar	1397
Instalar hardware	1401
Configurar software	1410
Redefinir o switch do cluster 3132Q-V para os padrões de fábrica	1473
Migrar switches	1473
Substitua os interruptores	1497
Cisco Nexus 92300YC	1543
Começar	1543
Instalar hardware	1548
Configurar o software	1561
Migrar switches	1601
Substitua os interruptores	1619
NetApp CN1610	1650
Visão geral da instalação e configuração dos switches NetApp CN1610	1650
Instalar e configurar o fluxo de trabalho para switches NetApp CN1610	1651
Requisitos de documentação para switches NetApp CN1610	1651
Instalar e configurar	1652
Migrar switches	1688
Substitua os interruptores	1716
Avisos legais	1742
Direitos autorais	1742
Marcas Registradas	1742
Patentes	1742
Política de Privacidade	1742

Documentação de switches para sistemas de armazenamento ONTAP

Começar

O que há de novo para switches?

Saiba mais sobre os novos switches para sistemas de armazenamento ONTAP. Para obter informações adicionais sobre os switches, consulte ["Hardware Universe"](#).

Novo suporte para interruptor

Interruptores	Descrição	Disponível a partir de
Switch Cisco de 32 portas 400GbE (X190300-CS-PI e X190300-PE)	Suporte para switch Cisco 9332D-GX2B Intra-Cluster/HA/Armazenamento.	ONTAP 9.17.1
Switch Cisco de 64 portas 400GbE (X190310-CS-PI)	Suporte para switch Cisco 9364D-GX2A Intra-Cluster/HA/Armazenamento.	ONTAP 9.17.1
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 10/25/40/100GbE e configurações de armazenamento 100GbE (armazenamento conectado ao switch).	ONTAP 9.10.1
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 10/25/40/100GbE e configurações de armazenamento 100GbE (armazenamento conectado ao switch).	ONTAP 9.10.1
Switch NVIDIA de 16 portas 100GbE (X190006-PE e X190006-PI)	Suporte para switch de interconexão de cluster NVIDIA SN2100 e switch de armazenamento, incluindo suporte para configurações de IP MetroCluster .	ONTAP 9.10.1
Switch Cisco de 36 portas 100GbE (X190200-CS-PE e X190200-CS-PI)	Suporta infraestrutura compartilhada (cluster, alta disponibilidade e armazenamento conectado ao switch) no mesmo par de switches Cisco Nexus 9336C-FX2, incluindo suporte para configurações IP MetroCluster .	ONTAP 9.9.1

Interruptores	Descrição	Disponível a partir de
Switch Cisco de 36 portas 100GbE (X190200-CS-PE e X190200-CS-PI), (X190210-FE-PE e X190210-FE-PI)	O switch de interconexão de cluster e switch de armazenamento Cisco Nexus 9336C-FX2 oferece suporte para sistemas de armazenamento AFF e ASA , bem como para conectividade de dados de front-end.	ONTAP 9.8
Switch Broadcom BES-53248 (X190005 e X190005R)	O switch de interconexão de cluster Broadcom BES-53248 oferece suporte a controladores AFF/ FAS com portas 10/25GbE e 40/100GbE.	ONTAP 9.8
Switch Cisco de 36 portas 100GbE (X190200) e switch Cisco de 32 portas 100GbE (X190100 e X190100R)	O switch de armazenamento Cisco Nexus 3232C oferece suporte para conectar os sistemas de armazenamento AFF e ASA com gavetas de unidades NVMe NS224: • AFF A800/ AFF ASA A800 • AFF A700/ AFF ASA A700 • AFF A400/ AFF ASA A400 • AFF A320	ONTAP 9.8

Saiba mais sobre sistemas AFX, cluster, armazenamento e switches compartilhados

A NetApp oferece sistemas AFX, cluster, armazenamento e switches compartilhados que fornecem comunicações internas com a capacidade de mover dados e interfaces de rede pelo cluster sem interrupções.

Os switches de "front-end" fornecem conectividade ao armazenamento do host, enquanto os switches de cluster de "back-end" fornecem conexões entre dois ou mais controladores NetApp .



Somente switches de back-end validados pela NetApp(encomendados à NetApp) são suportados.

Interruptores de sistemas AFX

Os switches de sistemas AFX permitem que você crie switches de rede rápidos, com baixo consumo de energia e que economizam espaço. Seu tamanho pequeno e alta densidade de portas os tornam ideais para lidar com grandes redes. As portas suportam diferentes velocidades e podem ser divididas em várias conexões. Os switches de sistemas AFX suportados pela NetApp incluem:

- Cisco Nexus 9332D-GX2B
- Cisco Nexus 9364D-GX2A

Comutadores de cluster

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

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

Interruptores de armazenamento

Os switches de armazenamento permitem rotear dados entre servidores e arrays de armazenamento em uma rede de área de armazenamento (SAN). Os switches de armazenamento compatíveis com a NetApp incluem:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- 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 RCFs (Funções de Configuração de Cluster) compartilhadas para cluster e armazenamento. O switch compartilhado compatível com a NetApp é:

- Cisco Nexus 9336C-FX2

Interruptores de fim de disponibilidade

Para obter uma lista de switches que não estão mais disponíveis para compra, mas ainda são suportados, consulte ["Interruptores de fim de disponibilidade"](#).

Comece a usar os sistemas AFX, cluster, armazenamento e switches compartilhados

Para começar a usar os sistemas AFX, cluster, armazenamento e switches compartilhados, você instala componentes de hardware e configura seu switch.

A implantação do switch envolve o seguinte fluxo de trabalho.



Instale o hardware do switch

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

Interruptores de sistemas AFX	Comutadores de cluster	Interruptores de armazenamento	Switches compartilhados
• "Instalar o switch Cisco Nexus 9332D-GX2B" • "Instalar o switch Cisco Nexus 9364D-GX2A"	• "Instale o interruptor BES-53248." • "Instalar o switch Cisco Nexus 9336C-FX2" • "Instale o switch NVIDIA SN2100"	• "Instalar o switch Cisco Nexus 9336C-FX2" • "Instale o switch NVIDIA SN2100"	• "Instalar o switch Cisco Nexus 9336C-FX2"

2

Instale o sistema de armazenamento e as prateleiras de armazenamento.

Instale seu sistema de armazenamento e prateleiras no armário ou estante. Acesse as instruções de instalação e configuração para o modelo da sua plataforma.

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

3

Conecte os interruptores aos controladores por meio de cabos.

As instruções de instalação e configuração do sistema ONTAP incluem instruções para a conexão dos cabos das portas do controlador ao switch. No entanto, se precisar de listas de cabos e transceptores compatíveis, além de informações detalhadas sobre as portas de host do seu switch, acesse as instruções a seguir para o modelo do seu switch.

Interruptores de sistemas AFX	Comutadores de cluster	Interruptores de armazenamento	Switches compartilhados
"Cabeamento do switch Cisco Nexus 9332D-GX2B" "Cabeamento do switch Cisco Nexus 9364D-GX2A"	"Cabeamento do switch BES-53248" "Cabeamento do switch Cisco Nexus 9336C-FX2" "Cabeamento do switch NVIDIA SN2100"	"Cabeamento do switch Cisco Nexus 9336C-FX2" "Cabeamento do switch NVIDIA SN2100"	"Cabeamento do switch Cisco Nexus 9336C-FX2"

4

Configure o software do switch

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

Interruptores de sistemas AFX	Comutadores de cluster	Interruptores de armazenamento	Switches compartilhados
"Instalar software para switch Cisco Nexus 9332D-GX2B" "Instalar software para switch Cisco Nexus 9364D-GX2A"	"Instale o software para os switches BES-53248." "Instalar software para switch Cisco Nexus 9336C-FX2" "Instale o software para o switch NVIDIA SN2100."	"Instalar software para switch Cisco Nexus 9336C-FX2" "Instale o software para o switch NVIDIA SN2100."	"Instalar software para switch Cisco Nexus 9336C-FX2"

5

Configuração completa do sistema

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

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

6

Configuração completa do ONTAP

Após instalar e configurar os controladores e switches do seu sistema ONTAP , você deve concluir a configuração do seu armazenamento no ONTAP. Acesse as instruções a seguir de acordo com a sua configuração de implantação.

- Para implantações do ONTAP , consulte ["Configurar ONTAP"](#) .
- Para implantações do ONTAP com MetroCluster , consulte ["Configure o Metrocluster com o ONTAP"](#) .

Interruptores de sistemas AFX

Cisco Nexus 9332D-GX2B

Começar

Fluxo de trabalho de instalação e configuração para switches Cisco 9332D-GX2B

O switch Cisco 9332D-GX2B faz parte da plataforma Cisco Nexus 9000. Os switches dos sistemas AFX permitem que você crie clusters ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches Cisco 9332D-GX2B.

1

"Revise os detalhes da porta do switch"

Revise os detalhes da porta do switch Cisco 9332D-GX2B.

2

"Revise a documentação necessária"

Revise a documentação específica do switch e do controlador para configurar seus switches 9332D-GX2B e o cluster ONTAP .

3

"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.

4

"Instale o hardware"

Instale o hardware do switch.

5

"Configurar o software"

Configure o software do switch.

Detalhes da porta para switches Cisco Nexus 9332D-GX2B

O switch Cisco Nexus 9332D-GX2B faz parte da plataforma Cisco Nexus 9000. Os switches do sistema AFX permitem que você crie clusters ONTAP com mais de dois nós.

Detalhes da porta Cisco Nexus 9332D-GX2B

Portos	Descrição
Ethernet1/1/1-4 para Ethernet1/30/1-4	Modo 4x100GbE para conexões de cluster, HA e armazenamento

Portos	Descrição
Ethernet 1/31, Ethernet 1/32	400GbE ISL

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Requisitos de documentação para switches Cisco Nexus 9332D-GX2B

Para a instalação do switch Cisco Nexus 9332D-GX2B, certifique-se de revisar a documentação específica do switch e do controlador para configurar seus switches 9332D-GX2B e o cluster ONTAP.

Documentação do Switch

Para configurar os switches Cisco Nexus 9332D-GX2B, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 9000"](#).

Título do documento	Descrição
"Guia de instalação de hardware do switch Cisco Nexus 9332D-GX2B NX-OS Mode"	Fornecer informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
"Guias de configuração de software para switches Cisco Nexus série 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornecer as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
"Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornecer informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
"Guia de Comandos do Cisco Nexus Série 9000 NX-OS"	Fornecer links para as diversas referências de comandos disponibilizadas pela Cisco.
"Referência de mensagens do sistema Cisco Nexus 9000 Series NX-OS"	Descrever as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.

Título do documento	Descrição
"Notas de versão do NX-OS para a série Cisco Nexus 9000" (Selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.
"Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000"	Fornecer informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 9000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
"Documentação dos sistemas AFX"	Descreve como instalar o hardware da NetApp .
"Documentação do ONTAP"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornecer informações sobre configuração e compatibilidade de hardware da NetApp .

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar hardware

Vá para o ["Fluxo de trabalho de instalação e configuração do AFX"](#) Para aprender como instalar e configurar o hardware do switch e o hardware do controlador para o seu sistema.

A documentação de instalação e configuração do AFX inclui informações como:

- Instruções para preparar o local, desembalar as caixas e comparar o conteúdo das caixas com a nota fiscal, além de registrar o sistema para acessar os benefícios de suporte.
- Instruções para instalar switches, controladores e prateleira de armazenamento em um gabinete NetApp ou rack de telecomunicações.
- Instruções para cabear seu sistema, incluindo cabeamento do armazenamento do controlador para conexões de switch e cabeamento da prateleira para conexões de switch.

Configurar software

Configurar fluxo de trabalho de software para switches Cisco 9332D-GX2B

Para instalar e configurar o software para um switch Cisco 9332D-GX2B e instalar ou atualizar o Arquivo de Configuração de Referência (RCF), siga estas etapas:

1

["Configurar o switch 9332D-GX2B"](#)

Configure o switch Cisco 9332D-GX2B.

2

["Prepare-se para instalar o software NX-OS e o RCF."](#)

Instale o software Cisco NX-OS e os arquivos de configuração de referência (RCFs) nos switches Cisco 9332D-GX2B.

3

["Instale ou atualize o software NX-OS."](#)

Baixe e instale ou atualize o software NX-OS no switch Cisco 9332D-GX2B.

4

["Instale ou atualize o RCF"](#)

Instale ou atualize o RCF após configurar o switch Cisco 9332D-GX2B pela primeira vez. Você também pode usar este procedimento para atualizar sua versão do RCF.

5

["Verifique se o SSH está habilitado nos switches Cisco 9332D-GX2B"](#)

Verifique se o SSH está habilitado no switch Cisco 9332D-GX2B para uso com o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

Após concluir a configuração dos seus switches, acesse ["Ligue seu sistema de armazenamento AFX 1K"](#) .

Configurar o switch 9332D-GX2B

Siga este procedimento para configurar o switch Cisco Nexus 9332D-GX2B.

Antes de começar

Certifique-se de ter:

- Ligue seus interruptores.
- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.



- O NX-OS 10.4.2 é a única versão suportada para switches Cisco Nexus 9332D-GX2B em um cluster ONTAP .
- Não atualize ou faça downgrade da sua versão do NX-OS para uma versão não suportada; somente a 10.4.2 é suportada atualmente.

- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Os RCFs aplicáveis para redes compartilhadas e redes de gerenciamento da NetApp podem ser baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) . Todos os switches de rede compartilhada e de gerenciamento da Cisco vêm com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Execute uma configuração inicial dos switches de rede compartilhados.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .

Incitar	Resposta
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	Digite o nome do interruptor, que está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave, de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.
Configurar camada de interface padrão (L3/L2)	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado)	Responda com noshut . O padrão é noshut.

Incitar	Resposta
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso)	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
3. Verifique a versão nos switches de rede compartilhados e, se necessário, baixe a versão do software compatível com a NetApp para os switches a partir do site da NetApp. ["Download do software Cisco"](#) página.

O que vem a seguir?

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 Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do cluster LIF são:
 - node1-01_clus1 e node1-01_clus2 para node1-01
 - node1-02_clus1 e node1-02_clus2 para node1-02
 - node1-03_clus1 e node1-03_clus2 para node1-03
 - node1-04_clus1 e node1-04_clus2 para node1-04
- O `cluster1::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os

comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

3. Verifique o status administrativo e operacional de cada porto.

a. Portas de cluster

- i. Exiba quantas interfaces de interconexão de cluster estão configuradas em cada nó para cada switch:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
node1-02/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLM284504N6)	Ethernet1/16/2

```
N9K-C9332D-GX2B
```

```
e7b
```

```
cs1 (FDO2846056X)
```

```
Ethernet1/16/2
```

```
N9K-C9332D-GX2B
```

```
.
```

```
.
```

```
.
```

ii. Exibir os atributos da porta de rede:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000

```
healthy false
```

```
Node: node1-04
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy false						
e7b	Cluster	Cluster		up	9000	auto/100000
healthy false						

```
8 entries were displayed.
```

iii. Exibir informações sobre os LIFs do cluster:

```
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					
01	e7a	node1-01_clus1 true	up/up	169.254.36.44/16	node1-
01	e7b	node1-01_clus2 true	up/up	169.254.7.5/16	node1-
02	e7a	node1-02_clus1 true	up/up	169.254.197.206/16	node1-
02	e7b	node1-02_clus2 true	up/up	169.254.195.186/16	node1-
03	e7a	node1-03_clus1 true	up/up	169.254.192.49/16	node1-
03	e7b	node1-03_clus2 true	up/up	169.254.182.76/16	node1-
04	e7a	node1-04_clus1 true	up/up	169.254.59.49/16	node1-
04	e7b	node1-04_clus2 true	up/up	169.254.62.244/16	node1-

```
8 entries were displayed.
```

b. Portas HA

i. Exibir informações sobre as portas HA:

```
ha interconnect status show -node <node-name>
```


Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: e1b-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Exibir informações sobre as portas de armazenamento:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----

1.1

0	A	connected	false
1	A	connected	false
2	A	connected	false
3	A	connected	false
4	A	connected	false
5	A	connected	false
6	A	connected	false
7	A	connected	false
8	B	connected	false
9	B	connected	false
10	B	connected	false
11	B	connected	false
12	B	connected	false
13	B	connected	false
14	B	connected	false
15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

4. Verifique a conectividade das interfaces do cluster remoto.

- a. Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

node1-01				
	6/4/2025 03:13:33	-04:00	node1-01_clus2	node1-02_clus1
none				
	6/4/2025 03:13:34	-04:00	node1-01_clus2	node1-02_clus1
none				
node1-02				
	6/4/2025 03:13:33	-04:00	node1-02_clus2	node1-01_clus1
none				
	6/4/2025 03:13:34	-04:00	node1-02_clus2	node1-01_clus2
none				
.				
.				
.				

- b. Alternativamente, você pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
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)
```

5. Verifique se o comando de reversão automática está habilitado em todos os 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	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

8 entries were displayed.

O que vem a seguir?

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 no switch Nexus 9332D-GX2B.

Requisitos de revisão

Antes de começar

Verifique o seguinte:

- Conclua o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) .
- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- ["Página do switch Ethernet da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornece informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do LIF do cluster são node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 e node1-04_clus2.
- O `cluster1::*>` O prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.



- O NX-OS 10.4.2 é a única versão suportada para switches Cisco Nexus 9332D-GX2B em um cluster ONTAP .
- Não atualize ou faça downgrade da sua versão do NX-OS para uma versão não suportada; somente a 10.4.2 é suportada atualmente.

Passos

1. Conecte o switch à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```


Mostrar exemplo

```
cluster1::*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1-01/cdp				
C9332D-GX2B	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:34:78:d3)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:19:a2:59)	Ethernet1/16/2	-
	.			
	.			
	.			

4. Verifique o status administrativo e operacional de cada porto.

a. **Portas de cluster**

i. Verifique se todas as portas do cluster estão ativas e com status íntegro:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

ii. Verifique se todas as interfaces de cluster (LIFs) estão na porta principal:

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

Mostrar exemplo

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

Current Vserver	Logical Current Interface	Is Home	Status Admin/Oper	Network Address/Mask	Node

Cluster					
node1-01	node1-01_clus1	up/up	169.254.36.44/16		
e7a	true				
node1-01	node1-01_clus2	up/up	169.254.7.5/16		
e7b	true				
node1-02	node1-02_clus1	up/up	169.254.197.206/16		
e7a	true				
node1-02	node1-02_clus2	up/up	169.254.195.186/16		
e7b	true				
node1-03	node1-03_clus1	up/up	169.254.192.49/16		
e7a	true				
node1-03	node1-03_clus2	up/up	169.254.182.76/16		
e7b	true				
node1-04	node1-04_clus1	up/up	169.254.59.49/16		
e7a	true				
node1-04	node1-04_clus2	up/up	169.254.62.244/16		
e7b	true				

8 entries were displayed.

iii. 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 Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs1 (FLMXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.253
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Portas HA

- Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: e1b-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

.
.
.

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Desative a reversão automática nos LIFs do cluster. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 9332D-GX2B.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.10.4.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: root

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
root@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get    /code/nxos.10.4.2.bin  /bootflash/nxos.10.4.2.bin
/code/nxos.10.4.2.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.10.4.2.F.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.10.4.2.F.img  /bootflash/n9000-
epld.10.4.2.F.img
/code/n9000-epld.10.4.2.F.img  100% 161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão do software NX-OS em execução:

```
show version
```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, 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 01.14
NXOS: version 10.4(1) [Feature Release]
Host NXOS: version 10.4(1)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.1.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 10.4(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale a imagem do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.10.4.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.10.4.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image  
bootflash:/nxos.10.4.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image  
bootflash:/nxos.10.4.2.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	10.4 (1)	10.4 (2)
Yes			
1	bios	xx.xx.:xx.xx	xxx
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.

9. Verifique a nova versão do software NX-OS após a reinicialização do switch:

show version

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, 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 01.14
NXOS: version 10.4(2) [Feature Release]
Host NXOS: version 10.4(2)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.2.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```



```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 10.4(2)
```

```
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	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.10.4.2.F.img module all
```

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 de todas as portas no cluster.

a. Portas de cluster

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

ii. Verifique o estado de funcionamento do switch no cluster:

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

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

node1-02/cdp
      e10a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e10b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e11a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e11b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e1a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      e1b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      .
      .
      .
      e7a   cs1 (FLM284504N6)       Ethernet1/16/2
N9K-C9332D-GX2B
      e7b   cs2 (FDO2846056X)       Ethernet1/16/2
N9K-C9332D-GX2B

node1-01/cdp
      e10a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e10b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e11a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e11b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e1a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      e1b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/2
N9K-C9332D-GX2B
      e7b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/2
N9K-C9332D-GX2B
      .
```

```

.
.

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                Type                                Address
Model                                -----
-----
cs2 (FDOXXXXXXXXX)                   cluster-network                   10.228.137.233
N9K-C9332D-GX2B
    Serial Number: FDOXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)                   cluster-network                   10.228.137.253
N9K-C9332D-GX2B
    Serial Number: FLMXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

```

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```


Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)

Node: node1-02
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

13. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	false
node1-04	true	true	true

4 entries were displayed.

14. Repita as etapas 6 a 13 para instalar o software NX-OS e as imagens EPLD no switch cs1.

15. Ative a reversão automática nos LIFs do cluster.

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

16. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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				
e7a	node1-01_clus1	up/up	169.254.36.44/16	node1-01
	true			
e7b	node1-01_clus2	up/up	169.254.7.5/16	node1-01
	true			
e7a	node1-02_clus1	up/up	169.254.197.206/16	node1-02
	true			
e7b	node1-02_clus2	up/up	169.254.195.186/16	node1-02
	true			
e7a	node1-03_clus1	up/up	169.254.192.49/16	node1-03
	true			
e7b	node1-03_clus2	up/up	169.254.182.76/16	node1-03
	true			
e7a	node1-04_clus1	up/up	169.254.59.49/16	node1-04
	true			
e7b	node1-04_clus2	up/up	169.254.62.244/16	node1-04
	true			

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif-name>
```

O que vem a seguir?

Após instalar ou atualizar o software NX-OS, você [instalar ou atualizar o arquivo de configuração de](#)

[referência \(RCF\)](#)" .

Instale ou atualize o RCF

Visão geral da instalação ou atualização do arquivo de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar o switch Nexus 9332D-GX2B pela primeira vez. Você atualiza a versão do RCF quando já tem uma versão existente do arquivo RCF instalada no seu switch.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configuração RCF disponível

- **Cluster-HA-Storage AFX** - Todas as portas estão configuradas no modo breakout 4x100GbE, que oferece suporte universal a clusters de nós AFX, alta disponibilidade (HA), portas de armazenamento e portas de prateleira de armazenamento NX224. ISL de 400GbE entre switches. (*Cluster-HA-Storage AFX RCF_vxx.x*).

Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de banner e notas importantes no seu RCF. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

Documentação sugerida

- ["Switches Ethernet Cisco \(NSS\)"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 9000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do LIF do cluster são node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 e node1-04_clus2.
- O `cluster1::*>` O prompt indica o nome do cluster.

Consulte o ["Hardware Universe"](#) para verificar as portas corretas em sua plataforma.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

O que vem a seguir?

Depois de revisar o procedimento de instalação do RCF ou atualização do RCF, você ["instalar o RCF"](#) ou ["atualize seu RCF"](#) conforme necessário.

Instale o RCF

Você instala o RCF depois de configurar o switch Nexus 9332D-GX2B pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma conexão de console com o switch. A conexão com o console é opcional se você tiver acesso remoto ao switch.
- Os switches cs1 e cs2 estão ligados e a configuração inicial dos switches está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão desejada do NX-OS foi instalada.
- As conexões ISL entre os switches estão conectadas.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch cs1 usando SSH ou usando um console serial.
2. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado nos ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#) guides.

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória flash de inicialização no switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9332D-GX2B-RCF-v10.0-Shared.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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado nos ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#) guides.

Este exemplo mostra o arquivo RCF. NX9332D-GX2B-RCF-v10.0-Shared.txt sendo instalado no switch cs1:

```
cs1# copy NX9332D-GX2B-RCF-v10.0-Shared.txt running-config echo-commands
```

4. Examine a saída do banner do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

Mostrar exemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : NX9332D-GX2B
* Filename    : NX9332D-GX2B-RCF-v10.0-Shared.txt
* Date       : 05-09-2025
* Version    : v10.0
* Port Usage:
* Ports 1-30: 100GbE Intra-Cluster/HA/Storage Ports, int e1/{1-
30}/1-4
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* Interface port-channel999 is reserved to identify the version of
this file.
*****
*****
```

5. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.

Certifique-se de configurar o seguinte:



- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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

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 1536" >>
bootflash:write_erase.cfg
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

7. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Emita 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
```

9. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Reinicie o switch:

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

11. Repita os passos 1 a 10 no switch cs2.

12. Conecte as portas de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch conectadas às portas do cluster estão ativas:

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1          eth  trunk  up      none
100G(D) --
Eth1/9/4          1          eth  trunk  up      none
100G(D) --
Eth1/15/1         1          eth  trunk  up      none
100G(D) --
Eth1/15/2         1          eth  trunk  up      none
100G(D) --
Eth1/15/3         1          eth  trunk  up      none
100G(D) --
Eth1/15/4         1          eth  trunk  up      none
100G(D) --
Eth1/16/1         1          eth  trunk  up      none
100G(D) --
Eth1/16/2         1          eth  trunk  up      none
100G(D) --
Eth1/16/3         1          eth  trunk  up      none
100G(D) --
Eth1/16/4         1          eth  trunk  up      none
100G(D) --
Eth1/17/1         1          eth  trunk  up      none
100G(D) --
Eth1/17/2         1          eth  trunk  up      none
100G(D) --
Eth1/17/3         1          eth  trunk  up      none
100G(D) --
Eth1/17/4         1          eth  trunk  up      none
100G(D) --
.
.
```

2. Verifique se os nós do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/1/1, Eth1/1/2, Eth1/1/3, Eth1/1/4, Eth1/2/1, Eth1/2/2, Eth1/2/3, Eth1/2/4, Eth1/3/1, Eth1/3/2, Eth1/3/3, Eth1/3/4, Eth1/4/1, Eth1/4/2, Eth1/4/3, Eth1/4/4, Eth1/5/1, Eth1/5/2, Eth1/5/3, Eth1/5/4, Eth1/6/1, Eth1/6/2, Eth1/6/3, Eth1/6/4, Eth1/7/1, Eth1/7/2, Eth1/7/3, Eth1/7/4, Eth1/8/1, Eth1/8/2, Eth1/8/3, Eth1/8/4, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4, Eth1/11/1, Eth1/11/2, Eth1/11/3, Eth1/11/4, Eth1/12/1, Eth1/12/2, Eth1/12/3, Eth1/12/4, Eth1/13/1, Eth1/13/2, Eth1/13/3, Eth1/13/4, Eth1/14/1, Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2		Eth1/14/4,
Eth1/15/4, Eth1/16/1		Eth1/15/3,
Eth1/16/3, Eth1/16/4		Eth1/16/2,
Eth1/17/2, Eth1/17/3		Eth1/17/1,
Eth1/18/1, Eth1/18/2		Eth1/17/4,
Eth1/18/4, Eth1/19/1		Eth1/18/3,
Eth1/19/3, Eth1/19/4		Eth1/19/2,
Eth1/20/2, Eth1/20/3		Eth1/20/1,
Eth1/21/1, Eth1/21/2		Eth1/20/4,
Eth1/21/4, Eth1/22/1		Eth1/21/3,
Eth1/22/3, Eth1/22/4		Eth1/22/2,
Eth1/23/2, Eth1/23/3		Eth1/23/1,
Eth1/24/1, Eth1/24/2		Eth1/23/4,
Eth1/24/4, Eth1/25/1		Eth1/24/3,
Eth1/25/3, Eth1/25/4		Eth1/25/2,
Eth1/26/2, Eth1/26/3		Eth1/26/1,
Eth1/27/1, Eth1/27/2		Eth1/26/4,
Eth1/27/4, Eth1/28/1		Eth1/27/3,
Eth1/28/3, Eth1/28/4		Eth1/28/2,
Eth1/29/2, Eth1/29/3		Eth1/29/1,
Eth1/30/1, Eth1/30/2		Eth1/29/4,
17 VLAN0017	active	Eth1/30/3, Eth1/30/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
		Eth1/1/4, Eth1/2/1,

Eth1/2/2	Eth1/2/3, Eth1/2/4,
Eth1/3/1	Eth1/3/2, Eth1/3/3,
Eth1/3/4	Eth1/4/1, Eth1/4/2,
Eth1/4/3	Eth1/4/4, Eth1/5/1,
Eth1/5/2	Eth1/5/3, Eth1/5/4,
Eth1/6/1	Eth1/6/2, Eth1/6/3,
Eth1/6/4	Eth1/7/1, Eth1/7/2,
Eth1/7/3	Eth1/7/4, Eth1/8/1,
Eth1/8/2	Eth1/8/3, Eth1/8/4,
Eth1/9/1	Eth1/9/2, Eth1/9/3,
Eth1/9/4	Eth1/10/1,
Eth1/10/2, Eth1/10/3	Eth1/10/4,
Eth1/11/1, Eth1/11/2	Eth1/11/3,
Eth1/11/4, Eth1/12/1	Eth1/12/2,
Eth1/12/3, Eth1/12/4	Eth1/13/1,
Eth1/13/2, Eth1/13/3	Eth1/13/4,
Eth1/14/1, Eth1/14/2	Eth1/14/3,
Eth1/14/4, Eth1/15/1	Eth1/15/2,
Eth1/15/3, Eth1/15/4	Eth1/16/1,
Eth1/16/2, Eth1/16/3	Eth1/16/4,
Eth1/17/1, Eth1/17/2	Eth1/17/3,
Eth1/17/4, Eth1/18/1	Eth1/18/2,
Eth1/18/3, Eth1/18/4	Eth1/19/1,

Eth1/19/2, Eth1/19/3		Eth1/19/4,
Eth1/20/1, Eth1/20/2		Eth1/20/3,
Eth1/20/4, Eth1/21/1		Eth1/21/2,
Eth1/21/3, Eth1/21/4		Eth1/22/1,
Eth1/22/2, Eth1/22/3		Eth1/22/4,
Eth1/23/1, Eth1/23/2		Eth1/23/3,
Eth1/23/4, Eth1/24/1		Eth1/24/2,
Eth1/24/3, Eth1/24/4		Eth1/25/1,
Eth1/25/2, Eth1/25/3		Eth1/25/4,
Eth1/26/1, Eth1/26/2		Eth1/26/3,
Eth1/26/4, Eth1/27/1		Eth1/27/2,
Eth1/27/3, Eth1/27/4		Eth1/28/1,
Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
18 VLAN0018	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,

Eth1/6/4	Eth1/7/1, Eth1/7/2,
Eth1/7/3	Eth1/7/4, Eth1/8/1,
Eth1/8/2	Eth1/8/3, Eth1/8/4,
Eth1/9/1	Eth1/9/2, Eth1/9/3,
Eth1/9/4	Eth1/10/1,
Eth1/10/2, Eth1/10/3	Eth1/10/4,
Eth1/11/1, Eth1/11/2	Eth1/11/3,
Eth1/11/4, Eth1/12/1	Eth1/12/2,
Eth1/12/3, Eth1/12/4	Eth1/13/1,
Eth1/13/2, Eth1/13/3	Eth1/13/4,
Eth1/14/1, Eth1/14/2	Eth1/14/3,
Eth1/14/4, Eth1/15/1	Eth1/15/2,
Eth1/15/3, Eth1/15/4	Eth1/16/1,
Eth1/16/2, Eth1/16/3	Eth1/16/4,
Eth1/17/1, Eth1/17/2	Eth1/17/3,
Eth1/17/4, Eth1/18/1	Eth1/18/2,
Eth1/18/3, Eth1/18/4	Eth1/19/1,
Eth1/19/2, Eth1/19/3	Eth1/19/4,
Eth1/20/1, Eth1/20/2	Eth1/20/3,
Eth1/20/4, Eth1/21/1	Eth1/21/2,
Eth1/21/3, Eth1/21/4	Eth1/22/1,
Eth1/22/2, Eth1/22/3	Eth1/22/4,
Eth1/23/1, Eth1/23/2	Eth1/23/3,

Eth1/23/4, Eth1/24/1		Eth1/24/2,
Eth1/24/3, Eth1/24/4		Eth1/25/1,
Eth1/25/2, Eth1/25/3		Eth1/25/4,
Eth1/26/1, Eth1/26/2		Eth1/26/3,
Eth1/26/4, Eth1/27/1		Eth1/27/2,
Eth1/27/3, Eth1/27/4		Eth1/28/1,
Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
30 VLAN0030	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
40 VLAN0040	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,
Eth1/11/1, Eth1/11/2		Eth1/11/3,
Eth1/11/4, Eth1/12/1		Eth1/12/2,
Eth1/12/3, Eth1/12/4		Eth1/13/1,
Eth1/13/2, Eth1/13/3		Eth1/13/4,
Eth1/14/1, Eth1/14/2		Eth1/14/3,
Eth1/14/4, Eth1/15/1		Eth1/15/2,

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

cs1# **show interface trunk**

```
-----  
-----  
Port          Native  Status          Port
```

	Vlan	Channel	

Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/30/1	none		
Eth1/30/2	none		
Eth1/30/3	none		
Eth1/30/4	none		
Eth1/31	none		
Eth1/32	none		
Po1	1		



Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

3. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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)
999    Po999 (SD)    Eth      NONE      --
cs1#
```

Etapa 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager oferece um fluxo de trabalho simples e fácil para a configuração e instalação de clusters, incluindo a atribuição de um endereço IP de gerenciamento de nó, a inicialização do cluster, a criação de uma camada local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Vá para ["Configurar o ONTAP em um novo cluster com o System Manager"](#) Para obter instruções de configuração.

O que vem a seguir?

Depois de instalar o RCF, você ["verificar a configuração SSH"](#).

Atualize sua versão do RCF

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapas 1: Prepare-se para a atualização

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exiba as portas em cada nó que estão conectadas aos switches:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1-01/cdp				
C9332D-GX2B	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
	.			
	.			
	.			
C9332D-GX2B	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/2	-

4. Verifique o status administrativo e operacional de cada porto.

a. **Portas de cluster**

- i. Verifique se todas as portas do cluster estão ativas e com status íntegro:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

ii. Verifique se todas as interfaces de cluster (LIFs) estão na porta principal:

```
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			
	node1-01_clus1	up/up	169.254.3.4/23
node1-01	e7a true		
	node1-01_clus2	up/up	169.254.3.5/23
node1-01	e7b true		
	node1-02_clus1	up/up	169.254.3.8/23
node1-02	e7a true		
	node1-02_clus2	up/up	169.254.3.9/23
node1-02	e7b true		
	node1-03_clus1	up/up	169.254.1.3/23
node1-03	e7a true		
	node1-03_clus2	up/up	169.254.1.1/23
node1-03	e7b true		
	node1-04_clus1	up/up	169.254.1.6/23
node1-04	e7a true		
	node1-04_clus2	up/up	169.254.1.7/23
node1-04	e7b true		
8 entries were displayed.			

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

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

Mostrar exemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs2 (FLMXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.234
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Portas HA

- Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: elb-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```


Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Desative a reversão automática nos LIFs do cluster.

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

Etapa 2: Configurar portas

1. No switch cs1, desligue as portas conectadas a todas as portas dos nós.

```

cs1# config
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,e1/7/1-4,e1/8/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-
4,e1/14/1-4,e1/15/1-4,e1/16/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-
4,e1/22/1-44,e1/23/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/24/1-,e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-
4,e1/29/1-4,e1/30/1-44
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit

```



Certifique-se de desativar **todas** as portas conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) para obter mais detalhes.

2. Verifique se os LIFs do cluster falharam nas portas hospedadas no switch 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				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			
8 entries were displayed.				

3. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
node1-01       true   true        false
node1-02       true   true        false
node1-03       true   true         true
node1-04       true   true        false

4 entries were displayed.
```

4. Caso ainda não o tenha feito, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

```
show running-config
```

- Registre quaisquer adições personalizadas entre o atual `running-config` e o arquivo RCF em uso (como uma configuração SNMP para sua organização).
 - Para NX-OS 10.2 e versões posteriores, use o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, use uma ferramenta de comparação/diferenciação de terceiros.
5. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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
```

```
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 1536" >>
```

```
bootflash:write_erase.cfg
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

6. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

7. Emita 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
```

8. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

9. Reinicie o switch:

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

10. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

11. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado nos ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#) guides.

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória flash de inicialização no switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9332D-GX2B-RCF-v10.0-Shared.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)...
```

12. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado nos ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#) guides.

Este exemplo mostra o arquivo RCF. `NX9332D-GX2B-RCF-v10.0-Shared.txt` sendo instalado no switch `cs1`:

```
cs1# copy NX9332D-GX2B-RCF-v10.0-Shared.txt running-config echo-commands
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

13. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

14. Reaplique quaisquer personalizações anteriores à configuração do switch.
15. Após verificar se as versões do RCF, as adições personalizadas e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado nos ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#) guides.

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

16. Reinicie o interruptor `cs1`. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e os eventos de "portas de cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

17. Verifique a integridade de todas as portas no cluster.

a. **Portas de cluster**

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do

cluster:

```
network port show -ip space 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					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8 entries were displayed.

ii. Verifique o estado de saúde do switch no cluster.

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

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4 (2)		

```
Version Source: CDP/ISDP
```

```
cs1 (FLMXXXXXXXX)          cluster-network    10.228.137.234  
N9K-C9332D-GX2B
```

```
    Serial Number: FLMXXXXXXXX
```

```
    Is Monitored: true
```

```
        Reason: None
```

```
    Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version
```

```
10.4(2)
```

```
Version Source: CDP/ISDP
```

```
2 entries were displayed.
```

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)

Node: node1-02
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

18. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

19. Repita os passos 4 a 18 no switch cs2.

20. Ative a reversão automática nos LIFs do cluster.

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

Etapa 3: Verifique a configuração de rede do cluster e a integridade do cluster.

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
show interface brief
```


Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1          eth  trunk  up      none
100G(D)  --
Eth1/9/4          1          eth  trunk  up      none
100G(D)  --
Eth1/15/1         1          eth  trunk  up      none
100G(D)  --
Eth1/15/2         1          eth  trunk  up      none
100G(D)  --
Eth1/15/3         1          eth  trunk  up      none
100G(D)  --
Eth1/15/4         1          eth  trunk  up      none
100G(D)  --
Eth1/16/1         1          eth  trunk  up      none
100G(D)  --
Eth1/16/2         1          eth  trunk  up      none
100G(D)  --
Eth1/16/3         1          eth  trunk  up      none
100G(D)  --
Eth1/16/4         1          eth  trunk  up      none
100G(D)  --
Eth1/17/1         1          eth  trunk  up      none
100G(D)  --
Eth1/17/2         1          eth  trunk  up      none
100G(D)  --
Eth1/17/3         1          eth  trunk  up      none
100G(D)  --
Eth1/17/4         1          eth  trunk  up      none
100G(D)  --
.
.
.
```

2. Verifique se os nós esperados ainda estão conectados:

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs2 (FDOXXXXXXXXX) Eth1/63	Eth1/31	179	R S I s	N9K-C9364D-GX2A
cs2 (FDOXXXXXXXXX) Eth1/64	Eth1/32	179	R S I s	N9K-C9364D-GX2A
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K
node1-02 e7a	Eth1/9/2	138	H	AFX-1K
node1-02 e10a	Eth1/9/3	138	H	AFX-1K
node1-02 e11a	Eth1/9/4	138	H	AFX-1K
node1-03 e1a	Eth1/15/1	138	H	AFX-1K
node1-03 e7a	Eth1/15/2	138	H	AFX-1K
node1-03 e10a	Eth1/15/3	138	H	AFX-1K
node1-03 e11a	Eth1/15/4	138	H	AFX-1K
node1-04 e1a	Eth1/16/1	173	H	AFX-1K
node1-04 e7a	Eth1/16/2	173	H	AFX-1K
node1-04 e10a	Eth1/16/3	173	H	AFX-1K
node1-04	Eth1/16/4	173	H	AFX-1K

```
e11a
```

```
Total entries displayed: 18
```

3. Verifique se os nós do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/1/1 Eth1/1/2, Eth1/1/3, Eth1/1/4 Eth1/2/1, Eth1/2/2, Eth1/2/3 Eth1/2/4, Eth1/3/1, Eth1/3/2 Eth1/3/3, Eth1/3/4, Eth1/4/1 Eth1/4/2, Eth1/4/3, Eth1/4/4 Eth1/5/1, Eth1/5/2, Eth1/5/3 Eth1/5/4, Eth1/6/1, Eth1/6/2 Eth1/6/3, Eth1/6/4, Eth1/7/1 Eth1/7/2, Eth1/7/3, Eth1/7/4 Eth1/8/1, Eth1/8/2, Eth1/8/3 Eth1/8/4, Eth1/9/1, Eth1/9/2 Eth1/9/3, Eth1/9/4, Eth1/10/1 Eth1/10/2, Eth1/10/3, Eth1/10/4 Eth1/11/1, Eth1/11/2, Eth1/11/3 Eth1/11/4, Eth1/12/1, Eth1/12/2 Eth1/12/3, Eth1/12/4, Eth1/13/1 Eth1/13/2, Eth1/13/3, Eth1/13/4 Eth1/14/1,

Eth1/14/2, Eth1/14/3		Eth1/14/4,
Eth1/15/1, Eth1/15/2		Eth1/15/3,
Eth1/15/4, Eth1/16/1		Eth1/16/2,
Eth1/16/3, Eth1/16/4		Eth1/17/1,
Eth1/17/2, Eth1/17/3		Eth1/17/4,
Eth1/18/1, Eth1/18/2		Eth1/18/3,
Eth1/18/4, Eth1/19/1		Eth1/19/2,
Eth1/19/3, Eth1/19/4		Eth1/20/1,
Eth1/20/2, Eth1/20/3		Eth1/20/4,
Eth1/21/1, Eth1/21/2		Eth1/21/3,
Eth1/21/4, Eth1/22/1		Eth1/22/2,
Eth1/22/3, Eth1/22/4		Eth1/23/1,
Eth1/23/2, Eth1/23/3		Eth1/23/4,
Eth1/24/1, Eth1/24/2		Eth1/24/3,
Eth1/24/4, Eth1/25/1		Eth1/25/2,
Eth1/25/3, Eth1/25/4		Eth1/26/1,
Eth1/26/2, Eth1/26/3		Eth1/26/4,
Eth1/27/1, Eth1/27/2		Eth1/27/3,
Eth1/27/4, Eth1/28/1		Eth1/28/2,
Eth1/28/3, Eth1/28/4		Eth1/29/1,
Eth1/29/2, Eth1/29/3		Eth1/29/4,
Eth1/30/1, Eth1/30/2		Eth1/30/3, Eth1/30/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		

Eth1/2/2	Eth1/1/4, Eth1/2/1,
Eth1/3/1	Eth1/2/3, Eth1/2/4,
Eth1/3/4	Eth1/3/2, Eth1/3/3,
Eth1/4/3	Eth1/4/1, Eth1/4/2,
Eth1/5/2	Eth1/4/4, Eth1/5/1,
Eth1/6/1	Eth1/5/3, Eth1/5/4,
Eth1/6/4	Eth1/6/2, Eth1/6/3,
Eth1/7/3	Eth1/7/1, Eth1/7/2,
Eth1/8/2	Eth1/7/4, Eth1/8/1,
Eth1/9/1	Eth1/8/3, Eth1/8/4,
Eth1/9/4	Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3	Eth1/10/1,
Eth1/11/1, Eth1/11/2	Eth1/10/4,
Eth1/11/4, Eth1/12/1	Eth1/11/3,
Eth1/12/3, Eth1/12/4	Eth1/12/2,
Eth1/13/2, Eth1/13/3	Eth1/13/1,
Eth1/14/1, Eth1/14/2	Eth1/13/4,
Eth1/14/4, Eth1/15/1	Eth1/14/3,
Eth1/15/3, Eth1/15/4	Eth1/15/2,
Eth1/16/2, Eth1/16/3	Eth1/16/1,
Eth1/17/1, Eth1/17/2	Eth1/16/4,
Eth1/17/4, Eth1/18/1	Eth1/17/3,
Eth1/18/3, Eth1/18/4	Eth1/18/2,

Eth1/19/2, Eth1/19/3		Eth1/19/1,
Eth1/20/1, Eth1/20/2		Eth1/19/4,
Eth1/20/4, Eth1/21/1		Eth1/20/3,
Eth1/21/3, Eth1/21/4		Eth1/21/2,
Eth1/22/2, Eth1/22/3		Eth1/22/1,
Eth1/23/1, Eth1/23/2		Eth1/22/4,
Eth1/23/4, Eth1/24/1		Eth1/23/3,
Eth1/24/3, Eth1/24/4		Eth1/24/2,
Eth1/25/2, Eth1/25/3		Eth1/25/1,
Eth1/26/1, Eth1/26/2		Eth1/25/4,
Eth1/26/4, Eth1/27/1		Eth1/26/3,
Eth1/27/3, Eth1/27/4		Eth1/27/2,
Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
18 VLAN0018	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		

Eth1/6/4

Eth1/7/3

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/6/2, Eth1/6/3,

Eth1/7/1, Eth1/7/2,

Eth1/7/4, Eth1/8/1,

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/4, Eth1/24/1		Eth1/23/3,
Eth1/24/3, Eth1/24/4		Eth1/24/2,
Eth1/25/2, Eth1/25/3		Eth1/25/1,
Eth1/26/1, Eth1/26/2		Eth1/25/4,
Eth1/26/4, Eth1/27/1		Eth1/26/3,
Eth1/27/3, Eth1/27/4		Eth1/27/2,
Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
30 VLAN0030	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		

Eth1/11/1, Eth1/11/2
Eth1/11/4, Eth1/12/1
Eth1/12/3, Eth1/12/4
Eth1/13/2, Eth1/13/3
Eth1/14/1, Eth1/14/2
Eth1/14/4, Eth1/15/1
Eth1/15/3, Eth1/15/4
Eth1/16/2, Eth1/16/3
Eth1/17/1, Eth1/17/2
Eth1/17/4, Eth1/18/1
Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4

Eth1/10/4,
Eth1/11/3,
Eth1/12/2,
Eth1/13/1,
Eth1/13/4,
Eth1/14/3,
Eth1/15/2,
Eth1/16/1,
Eth1/16/4,
Eth1/17/3,
Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,

Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
40 VLAN0040	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,
Eth1/11/1, Eth1/11/2		Eth1/11/3,
Eth1/11/4, Eth1/12/1		Eth1/12/2,
Eth1/12/3, Eth1/12/4		Eth1/13/1,
Eth1/13/2, Eth1/13/3		Eth1/13/4,
Eth1/14/1, Eth1/14/2		Eth1/14/3,
Eth1/14/4, Eth1/15/1		

Eth1/15/3, Eth1/15/4
Eth1/16/2, Eth1/16/3
Eth1/17/1, Eth1/17/2
Eth1/17/4, Eth1/18/1
Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4

Eth1/15/2,
Eth1/16/1,
Eth1/16/4,
Eth1/17/3,
Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/30/1	none		
Eth1/30/2	none		
Eth1/30/3	none		
Eth1/30/4	none		
Eth1/31	none		
Eth1/32	none		
Po1	1		



Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

4. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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)
999    Po999 (SD)     Eth      NONE      --
cs1#
```

5. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			

```
8 entries were displayed.
```

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver vservice_name -lif <lif-name>
```

6. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

7. Verifique a conectividade das interfaces do cluster remoto:

- Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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


Mostrar exemplo

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

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

node1-01				
	6/4/2025 03:13:33	-04:00	node1-01_clus2	node1-02_clus1
none				
	6/4/2025 03:13:34	-04:00	node1-01_clus2	node1-02_clus1
none				
node1-02				
	6/4/2025 03:13:33	-04:00	node1-02_clus2	node1-01_clus1
none				
	6/4/2025 03:13:34	-04:00	node1-02_clus2	node1-01_clus2
none				
.				
.				
.				

- b. Alternativamente, você pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
  Local 169.254.59.49 to Remote 169.254.192.49
  Local 169.254.59.49 to Remote 169.254.195.186
  Local 169.254.59.49 to Remote 169.254.197.206
  Local 169.254.59.49 to Remote 169.254.36.44
  Local 169.254.59.49 to Remote 169.254.7.5
  Local 169.254.62.244 to Remote 169.254.182.76
  Local 169.254.62.244 to Remote 169.254.192.49
  Local 169.254.62.244 to Remote 169.254.195.186
  Local 169.254.62.244 to Remote 169.254.197.206
  Local 169.254.62.244 to Remote 169.254.36.44
  Local 169.254.62.244 to Remote 169.254.7.5
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 vem a seguir?

Depois de atualizar seu RCF, você ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches.

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:Wed May 14 18:49:37 2025
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGCndfdJesautdCwk5Mk/7pKOF10IeShc9uBtj74  
F52vbjyf1FHOCXX7Xf3Vopxs6L1hbgzGpFLo9E7pZBd3I+1AoLyQUltR3svzNieGY8ml  
WZGLtpKf/P2fDCd8JVJaejrwQhm49WUPiC6ziEqBDMOGhJpD2e9++umyDdr6  
NbmK8Q==
```

```
bitcount:1024
```

```
fingerprint:
```

```
SHA256:QtNU+Qq2I4ZfYwEfMEB1+z8w7xaKTlantTdsjLBx+OU
```

```
could not retrieve dsa key information
```

```
ecdsa Keys generated:Wed May 14 18:50:56 2025
```

```
ecdsa-sha2-nistp521
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBAAAYnv17T+JlGmH8  
rg81xiOow0mPmkbkIG0o7h9EchixO3i3KjgQr8AwqkRHNTcQC3lRnizhJFUeMGCwuQTu  
rziRCwE6fAOkWa2MRyXA1DYRKKXjVEOnW9+MvinMipHQ0cCc  
YSExhh7j4HvWHIuYv8RmD7e3rmDQFlyyiLwdmpGfas2yaw==
```

```
bitcount:521
```

```
fingerprint:
```

```
SHA256:7cpZ5NGnIq5Iamw67ke+9o4qG9D3xxmGPauV14X5934
```

```
(switch)# show feature | include scpServer  
scpServer          1          enabled  
(switch)# show feature | include ssh  
sshServer          1          enabled  
(switch)#
```

O que vem a seguir?

Após verificar sua configuração SSH, você "[configurar monitoramento de integridade do switch](#)".

Redefinir o switch 9332D-GX2B para os padrões de fábrica

Para redefinir o switch 9332D-GX2B para os padrões de fábrica, você deve apagar as configurações do switch 9332D-GX2B.

Sobre esta tarefa

- Você precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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 um switch Cisco Nexus 9332D-GX2B

Siga estas etapas para substituir um switch Nexus 9332D-GX2B com defeito em uma rede compartilhada. Este é um procedimento não disruptivo (NDU).

Requisitos de revisão

Antes de substituir o interruptor, certifique-se de que:

- Você verificou o número de série do interruptor para garantir que o interruptor correto seja substituído.
- Na infraestrutura de cluster e rede existente:
 - O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
 - Todas as portas do cluster estão ativas.

- Todas as interfaces lógicas do cluster (LIFs) estão ativas e em suas portas de origem.
- O ONTAP `cluster ping-cluster -node <node-name>` O comando deve indicar que a conectividade básica e a comunicação com dispositivos maiores que PMTU estão funcionando corretamente em todos os caminhos.
- No switch de substituição Nexus 9332D-GX2B:
 - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - As conexões do nó são as portas 1/1 a 1/30.
 - Todas as portas Inter-Switch Link (ISL) estão desabilitadas nas portas 1/31 e 1/32.
 - O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional NX-OS são carregados no switch.
 - A personalização inicial do interruptor está concluída, conforme detalhado em ["Configurar o switch de cluster 9332D-GX2B"](#).

Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, são copiadas para o novo switch.
- Você executou o comando para migrar uma LIF de cluster do nó onde a LIF de cluster está hospedada.

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos switches Nexus 9332D-GX2B existentes são cs1 e cs2.
- O nome do novo switch Nexus 9332D-GX2B é newcs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do cluster LIF são node1-01_clus1 e node1-01_clus2 para node1-01, node1-02_clus1 e node1-02_clus2 para node1-02, node1-03_clus1 e node1-03_clus2 para node1-03 e node1-04_clus1 e node1-04_clus2 para node1-04.
- O prompt para alterações em todos os nós do cluster é `cluster1::*>`

Sobre esta tarefa

O procedimento a seguir baseia-se na seguinte topologia de rede em cluster:

Mostrar exemplo

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

Node: nodel-01

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	-----

e7a	Cluster	Cluster		up	9000	auto/100000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/100000	healthy
false							

Node: nodel-02

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	-----

e7a	Cluster	Cluster		up	9000	auto/100000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/100000	healthy
false							

Node: nodel-03

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	-----

e7a	Cluster	Cluster		up	9000	auto/100000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/100000	healthy

false

Node: node1-04

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	-----	-----	-----

e7a	Cluster	Cluster		up	9000	auto/100000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/100000	healthy
false							

8 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					
	node1-01_clus1	up/up	169.254.36.44/16	node1-01	e7a
true					
	node1-01_clus2	up/up	169.254.7.5/16	node1-01	e7b
true					
	node1-02_clus1	up/up	169.254.197.206/16	node1-02	e7a
true					
	node1-02_clus2	up/up	169.254.195.186/16	node1-02	e7b
true					
	node1-03_clus1	up/up	169.254.192.49/16	node1-03	e7a
true					
	node1-03_clus2	up/up	169.254.182.76/16	node1-03	e7b
true					
	node1-04_clus1	up/up	169.254.59.49/16	node1-04	e7a
true					
	node1-04_clus2	up/up	169.254.62.244/16	node1-04	e7b
true					

8 entries were displayed.


```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B				
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B				
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B				
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B				
	.			
	.			
	.			
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B				
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B				

```
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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
Device-ID Port ID					
cs2 (FDOXXXXXXXXX)	Eth1/31	179	R S I s	N9K-C9364D-GX2A	
Eth1/63					
cs2 (FDOXXXXXXXXX)	Eth1/32	179	R S I s	N9K-C9364D-GX2A	
Eth1/64					
node1-01	Eth1/4/1	123	H	AFX-1K	
e1a					
node1-01	Eth1/4/2	123	H	AFX-1K	
e7a					

node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				
node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

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					
Device-ID	Local Intrfce	Hldtme	Capability	Platform	
Port ID					
cs1 (FLMXXXXXXXX)	Eth1/31	179	R S I s	N9K-C9364D-GX2A	
Eth1/63					
cs1 (FLMXXXXXXXX)	Eth1/32	179	R S I s	N9K-C9364D-GX2A	
Eth1/64					

node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K
e7a				
node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				
node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

Etapa 1: Prepare-se para a substituição

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

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Instale o RCF e a imagem apropriados no switch, newcs2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e NX-OS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e NX-OS, continue para a etapa 2.

- a. Acesse a página *NetApp Cluster and Management Network Switches Reference Configuration File Description* no site de suporte da NetApp .
 - b. Clique no link para a *Matriz de Compatibilidade de Rede de Cluster e Rede de Gerenciamento* e, em seguida, observe a versão de software do switch necessária.
 - c. Clique na seta "Voltar" do seu navegador para retornar à página de Descrição, clique em **CONTINUAR**, aceite o contrato de licença e, em seguida, acesse a página de Download.
 - d. Siga os passos na página de Download para baixar os arquivos RCF e NX-OS corretos para a versão do software ONTAP que você está instalando.
3. No novo switch, efetue login como administrador e desligue todas as portas que serão conectadas às interfaces do cluster de nós (portas 1/1 a 1/30).

Se o interruptor que você está substituindo não estiver funcionando e estiver desligado, vá para a Etapa 4. As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em cada nó.

Mostrar exemplo

```
newcs2# config
newcs2(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,e1/7/1-4,e1/8/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-
4,e1/13/1-4,e1/14/1-4,e1/15/1-4,e1/16/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-
4,e1/21/1-4,e1/22/1-44,e1/23/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/24/1-,e1/25/1-4,e1/26/1-4,e1/27/1-
4,e1/28/1-4,e1/29/1-4,e1/30/1-44
newcs2(config-if-range)# shutdown
newcs2(config-if-range)# exit
newcs2(config)# exit
```

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
```

Vserver	Logical Interface	Auto-revert
Cluster	node1-01_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-04_clus2	true

```
4 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

- Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, você também pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
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 Eth1/31 e Eth1/32 no switch Nexus 9332D-GX2B cs1.

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/31-32
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
```

2. Remova todos os cabos do switch Nexus 9332D-GX2B cs2 e conecte-os às mesmas portas no switch 9332D-GX2B newcs2.
3. Abra as portas ISLs Eth1/31 e Eth1/32 entre os switches cs1 e newcs2 e, em seguida, verifique o status da operação do canal da porta.

Port-Channel deve indicar Po1(SU) e Member Ports deve indicar Eth1/31(P) e Eth1/32(P).

Mostrar exemplo

Este exemplo habilita as portas ISL Eth1/31 e Eth1/32 e exibe o resumo do canal de porta no switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/31-32
cs1(config-if-range)# no shutdown
cs1(config-if-range)# exit
cs1(config)# exit
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      Eth1/31 (P)  Eth1/32 (P)
999    Po999 (SD)    Eth      NONE      --
```

4. Verifique se a porta e7b está ativa em todos os nós:

```
network port show ipspace Cluster
```


Mostrar exemplo

O resultado deverá ser semelhante ao seguinte:

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

Node: node1-01

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-03

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	

```

healthy false
e7b          Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node1-04

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e7a        Cluster      Cluster      up    9000  auto/100000
healthy false
e7b        Cluster      Cluster      up    9000  auto/100000
healthy false

8 entries were displayed.

```

5. No mesmo nó usado na etapa anterior, reverta a LIF do cluster associada à porta da etapa anterior usando o comando `network interface revert`.

Mostrar exemplo

Neste exemplo, o LIF node1-01_clus2 no node1-01 é revertido com sucesso se o valor Home for verdadeiro e a porta for e7b.

Os seguintes comandos retornam LIF node1-01_clus2 sobre node1-01 para o porto de origem e7a e exibe informações sobre os LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se a coluna "Is Home" (É o nó principal) for verdadeira para ambas as interfaces do cluster e elas mostrarem as atribuições de porta corretas, neste exemplo. e7a e e7b no nó 1-01.

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7b	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7a	false			
	.			
	.			
	.			

6. Exibir informações sobre os nós em um cluster:

```
cluster show
```

Mostrar exemplo

Este exemplo mostra que o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1-01	false	true
node1-02	true	true
node1-03	true	true
node1-04	true	true

7. Verifique se todas as portas físicas do cluster estão ativas:

```
network port show ipspace Cluster
```

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

.
. .
. .

8. Verifique a conectividade das interfaces do cluster remoto:

- Você pode usar o `network interface check cluster-connectivity` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, você também pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
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. Verifique a integridade de todas as portas no cluster.

a. Portas de cluster

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

```
network port show ipspace Cluster
```

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

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

```
show cdp neighbors
```


Mostrar exemplo

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

```
Node: node1-01
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-02
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-03
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 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				
e7a	node1-01_clus1	up/up	169.254.209.69/16	node1-01
	true			
e7b	node1-01_clus2	up/up	169.254.49.125/16	node1-01
	true			
e7b	node1-02_clus1	up/up	169.254.47.194/16	node1-02
	true			
e7a	node1-02_clus2	up/up	169.254.19.183/16	node1-02
	true			
e7a	node1-03_clus1	up/up	169.254.209.69/16	node1-03
	true			
e7b	node1-03_clus2	up/up	169.254.49.125/16	node1-03
	true			
e7b	node1-04_clus1	up/up	169.254.47.194/16	node1-04
	true			
e7a	node1-04_clus2	up/up	169.254.19.183/16	node1-04
	false			

8 entries were displayed.

```
cluster1::> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	.		
	.		
	.		

```
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 Platform	Local Port	Intrfce ID	Hldtme	Capability	
newcs2 (FDOXXXXXXXXX)	Eth1/31		179	R S I s	N9K-
C9364D-GX2A	Eth1/63				
newcs2 (FDOXXXXXXXXX)	Eth1/32		179	R S I s	N9K-
C9364D-GX2A	Eth1/64				

nodel-01	Eth1/4/1	123	H	AFX-1K
e1a				
nodel-01	Eth1/4/2	123	H	AFX-1K
e7a				
nodel-01	Eth1/4/3	123	H	AFX-1K
e10a				
nodel-01	Eth1/4/4	123	H	AFX-1K
e11a				
nodel-02	Eth1/9/1	138	H	AFX-1K
e1a				
nodel-02	Eth1/9/2	138	H	AFX-1K
e7a				
nodel-02	Eth1/9/3	138	H	AFX-1K
e10a				
nodel-02	Eth1/9/4	138	H	AFX-1K
e11a				
nodel-03	Eth1/15/1	138	H	AFX-1K
e1a				
nodel-03	Eth1/15/2	138	H	AFX-1K
e7a				
nodel-03	Eth1/15/3	138	H	AFX-1K
e10a				
nodel-03	Eth1/15/4	138	H	AFX-1K
e11a				
nodel-04	Eth1/16/1	173	H	AFX-1K
e1a				
nodel-04	Eth1/16/2	173	H	AFX-1K
e7a				
nodel-04	Eth1/16/3	173	H	AFX-1K
e10a				
nodel-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

newcs2# **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 (FDOXXXXXXXXX) Eth1/31      179   R S I s   N9K-
C9364D-GX2A      Eth1/63
cs1 (FDOXXXXXXXXX) Eth1/32      179   R S I s   N9K-
C9364D-GX2A      Eth1/64
node1-01          Eth1/4/1      123   H          AFX-1K
e1a
node1-01          Eth1/4/2      123   H          AFX-1K
e7a
node1-01          Eth1/4/3      123   H          AFX-1K
e10a
node1-01          Eth1/4/4      123   H          AFX-1K
e11a
node1-02          Eth1/9/1      138   H          AFX-1K
e1a
node1-02          Eth1/9/2      138   H          AFX-1K
e7a
node1-02          Eth1/9/3      138   H          AFX-1K
e10a
node1-02          Eth1/9/4      138   H          AFX-1K
e11a
node1-03          Eth1/15/1     138   H          AFX-1K
e1a
node1-03          Eth1/15/2     138   H          AFX-1K
e7a
node1-03          Eth1/15/3     138   H          AFX-1K
e10a
node1-03          Eth1/15/4     138   H          AFX-1K
e11a
node1-04          Eth1/16/1     173   H          AFX-1K
e1a
node1-04          Eth1/16/2     173   H          AFX-1K
e7a
node1-04          Eth1/16/3     173   H          AFX-1K
e10a
node1-04          Eth1/16/4     173   H          AFX-1K
e11a

```

Total entries displayed: 18

b. Portas HA

i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```


Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você ["configurar monitoramento de integridade do switch"](#) .

Cisco Nexus 9364D-GX2A

Começar

Fluxo de trabalho de instalação e configuração para switches Cisco 9364D-GX2A

O switch Cisco 9364D-GX2A faz parte da plataforma Cisco Nexus 9000. Os switches de sistemas AFX permitem que você crie clusters ONTAP com mais de dois nós.

Siga estas etapas do fluxo de trabalho para instalar e configurar seus switches Cisco 9364D-GX2A.

1

"Revise os detalhes da porta do switch"

Revise os detalhes da porta do switch Cisco 9364D-GX2A.

2

"Revise a documentação necessária"

Revise a documentação específica do switch e do controlador para configurar seus switches 9364D-GX2A e o cluster ONTAP .

3

"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.

4

"Instale o hardware"

Instale o hardware do switch.

5

"Configurar o software"

Configure o software do switch.

Detalhes da porta para switches Cisco Nexus 9364D-GX2A

O switch Cisco Nexus 9364D-GX2A faz parte da plataforma Cisco Nexus 9000 e pode ser instalado em um gabinete de sistema NetApp . Os switches 9364D-GX2A permitem que você crie clusters ONTAP com mais de dois nós.

Detalhes da porta Cisco Nexus 9364D-GX2A

Portos	Descrição
Ethernet1/1/1-4 para Ethernet1/62/1-4	Modo 4x100GbE para cluster, HA, conexões de armazenamento AMD
Ethernet 1/63, Ethernet 1/64	400GbE ISL

Consulte o "[Hardware Universe](#)" para obter detalhes sobre as portas utilizadas pela plataforma.

Requisitos de documentação para switches Cisco Nexus 9364D-GX2A

Para a instalação do switch Cisco Nexus 9364D-GX2A, certifique-se de revisar a documentação específica do switch e do controlador para configurar seus switches Cisco 9364D-GX2A e o cluster ONTAP.

Documentação do Switch

Para configurar os switches Cisco Nexus 9364D-GX2A, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 9000"](#).

Título do documento	Descrição
"Guia de instalação de hardware do switch Cisco Nexus 9364D-GX2A NX-OS Mode"	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
"Guias de configuração de software para switches Cisco Nexus série 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
"Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
"Guia de Comandos do Cisco Nexus Série 9000 NX-OS"	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
"Referência de mensagens do sistema Cisco Nexus 9000 Series NX-OS"	Descreve as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
"Notas de versão do NX-OS para a série Cisco Nexus 9000" (Selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.
"Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000"	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 9000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
"Documentação dos sistemas AFX"	Descreve como instalar o hardware da NetApp .

Nome	Descrição
"Documentação do ONTAP"	Fornece informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornece informações sobre configuração e compatibilidade de hardware da NetApp .

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar hardware

Vá para o ["Fluxo de trabalho de instalação e configuração do AFX"](#) Para aprender como instalar e configurar o hardware do switch e o hardware do controlador para o seu sistema.

A documentação de instalação e configuração do AFX inclui informações como:

- Instruções para preparar o local, desembalar as caixas e comparar o conteúdo das caixas com a nota fiscal, além de registrar o sistema para acessar os benefícios de suporte.
- Instruções para instalar switches, controladores e prateleira de armazenamento em um gabinete NetApp ou rack de telecomunicações.
- Instruções para cabear seu sistema, incluindo cabeamento do armazenamento do controlador para conexões de switch e cabeamento da prateleira para conexões de switch.

Configurar software

Configurar fluxo de trabalho de software para switches Cisco 9364D-GX2A

Para instalar e configurar o software para um switch Cisco 9364D-GX2A e instalar ou atualizar o Arquivo de Configuração de Referência (RCF), siga estas etapas:

1

"Configurar o switch 9364D-GX2A"

Configure o switch Cisco 9364D-GX2A.

2

"Prepare-se para instalar o software NX-OS e o RCF."

Instale o software Cisco NX-OS e os arquivos de configuração de referência (RCFs) nos switches Cisco 9364D-GX2A.

3

"Instale ou atualize o software NX-OS."

Baixe e instale ou atualize o software NX-OS no switch Cisco 9364D-GX2A.

4

"Instale ou atualize o RCF"

Instale ou atualize o RCF após configurar o switch Cisco 9364D-GX2A pela primeira vez. Você também pode usar este procedimento para atualizar sua versão do RCF.

5

"Verifique se o SSH está habilitado nos switches Nexus 9364D-GX2A"

Verifique se o SSH está habilitado no switch Cisco 9364D-GX2A para uso com o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

Após concluir a configuração dos seus switches, acesse "[Ligue seu sistema de armazenamento AFX 1K](#)".

Configurar o switch 9364D-GX2A

Siga este procedimento para configurar o switch Cisco Nexus 9364D-GX2A.

Antes de começar

Certifique-se de ter:

- Ligue seus interruptores.
- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de "[Download do software Cisco](#)" página.



- O NX-OS 10.4.2 é a única versão suportada para switches Cisco Nexus 9364D-GX2A em um cluster ONTAP .
- Não atualize ou faça downgrade da sua versão do NX-OS para uma versão não suportada; somente a 10.4.2 é suportada atualmente.

- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em "meusuporte.netapp.com" . Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- "[Documentação necessária sobre switches e ONTAP](#)".

Passos

1. Realize uma configuração inicial dos switches de rede do cluster.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	Digite o nome do interruptor, que está limitado a 63 caracteres alfanuméricos.

Incitar	Resposta
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave, de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.
Configurar camada de interface padrão (L3/L2)	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado)	Responda com noshut . O padrão é noshut.
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso)	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.

Incitar	Resposta
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
3. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software compatível com a NetApp para os switches a partir do ["Download do software Cisco"](#) página.

O que vem a seguir?

Depois de configurar seus switches, você ["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 Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do cluster LIF são:
 - node1-01_clus1 e node1-01_clus2 para node1-01
 - node1-02_clus1 e node1-02_clus2 para node1-02
 - node1-03_clus1 e node1-03_clus2 para node1-03
 - node1-04_clus1 e node1-04_clus2 para node1-04
- O `cluster1::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

3. Verifique o status administrativo e operacional de cada porto.

- a. **Portas de cluster**

- i. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

node1-02/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2
N9K-C9364D-GX2A			
	e7b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/2
N9K-C9364D-GX2A			
node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2

```
N9K-C9364D-GX2A
```

```
e7b
```

```
cs2 (FDOXXXXXXXX)
```

```
Ethernet1/13/2
```

```
N9K-C9364D-GX2A
```

```
.
```

```
.
```

```
.
```

ii. Exibir os atributos da porta de rede:

```
network port show -ip space Cluster
```

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000

```
healthy false
```

```
Node: node1-04
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy false						
e7b	Cluster	Cluster		up	9000	auto/100000
healthy false						

```
8 entries were displayed.
```

iii. Exibir informações sobre os LIFs do cluster:

```
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					
01	e7a	node1-01_clus1 true	up/up	169.254.36.44/16	node1-
01	e7b	node1-01_clus2 true	up/up	169.254.7.5/16	node1-
02	e7a	node1-02_clus1 true	up/up	169.254.197.206/16	node1-
02	e7b	node1-02_clus2 true	up/up	169.254.195.186/16	node1-
03	e7a	node1-03_clus1 true	up/up	169.254.192.49/16	node1-
03	e7b	node1-03_clus2 true	up/up	169.254.182.76/16	node1-
04	e7a	node1-04_clus1 true	up/up	169.254.59.49/16	node1-
04	e7b	node1-04_clus2 true	up/up	169.254.62.244/16	node1-

```
8 entries were displayed.
```

b. Portas HA

i. Exibir informações sobre as portas HA:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: e1b-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

.
.
.

a. Portas de armazenamento

- i. Exibir informações sobre as portas de armazenamento:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----

1.1

0	A	connected	false
1	A	connected	false
2	A	connected	false
3	A	connected	false
4	A	connected	false
5	A	connected	false
6	A	connected	false
7	A	connected	false
8	B	connected	false
9	B	connected	false
10	B	connected	false
11	B	connected	false
12	B	connected	false
13	B	connected	false
14	B	connected	false
15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

4. Verifique a conectividade das interfaces do cluster remoto.

- a. Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none			
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none			
.			
.			
.			

- b. Alternativamente, você pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
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)
```

5. Verifique se o comando de reversão automática está habilitado em todos os 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	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

8 entries were displayed.

O que vem a seguir?

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 no switch Nexus 9364D-GX2A.

Requisitos de revisão

Antes de começar

Verifique o seguinte:

- Conclua o procedimento em "[Prepare-se para instalar o NX-OS e o RCF](#)".
- Um backup atual da configuração do switch está disponível.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes) está em vigor.

Documentação sugerida

- "[Página do switch Ethernet da Cisco](#)"

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- "[Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000](#)"

Fornece informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do LIF do cluster são node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 e node1-04_clus2.
- O `cluster1::*>` O prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.



- O NX-OS 10.4.2 é a única versão suportada para switches Cisco Nexus 9364D-GX2A em um cluster ONTAP .
- Não atualize ou faça downgrade da sua versão do NX-OS para uma versão não suportada; somente a 10.4.2 é suportada atualmente.

Passos

1. Conecte o switch à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

Mostrar exemplo



```
cluster1::*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/3	N9K-
C9364D-GX2A				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9364D-GX2A				
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/4	N9K-
C9364D-GX2A				
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9364D-GX2A				
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/1	N9K-
C9364D-GX2A				
	.			
	.			
	.			
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9364D-GX2A				
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/2	N9K-
C9364D-GX2A				
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/2	-
	.			
.				
.				
.				

4. Verifique o status administrativo e operacional de cada porto.

a. **Portas de cluster**

i. Verifique se todas as portas do cluster estão ativas e com status íntegro:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

ii. Verifique se todas as interfaces de cluster (LIFs) estão na porta principal:

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

Mostrar exemplo

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

Current Vserver Port	Logical Current Interface Home	Is	Status Admin/Oper	Network Address/Mask	Node

Cluster					
	node1-01_clus1		up/up	169.254.36.44/16	
node1-01	e7a	true			
	node1-01_clus2		up/up	169.254.7.5/16	
node1-01	e7b	true			
	node1-02_clus1		up/up	169.254.197.206/16	
node1-02	e7a	true			
	node1-02_clus2		up/up	169.254.195.186/16	
node1-02	e7b	true			
	node1-03_clus1		up/up	169.254.192.49/16	
node1-03	e7a	true			
	node1-03_clus2		up/up	169.254.182.76/16	
node1-03	e7b	true			
	node1-04_clus1		up/up	169.254.59.49/16	
node1-04	e7a	true			
	node1-04_clus2		up/up	169.254.62.244/16	
node1-04	e7b	true			

8 entries were displayed.

iii. 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 Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs1 (FLMXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.253
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Portas HA

- Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: elb-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)

Node: node1-02
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

.
.
.

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.1	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```


Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Desative a reversão automática nos LIFs do cluster. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 9364D-GX2A.

Mostrar exemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.10.4.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: root

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
root@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get    /code/nxos.10.4.2.bin    /bootflash/nxos.10.4.2.bin
/code/nxos.10.4.2.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.10.4.2.F.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.10.4.2.F.img    /bootflash/n9000-
epld.10.4.2.F.img
/code/n9000-epld.10.4.2.F.img  100% 161MB    9.5MB/s    00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique a versão do software NX-OS em execução:

```
show version
```

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, 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 01.14
NXOS: version 10.4(1) [Feature Release]
Host NXOS: version 10.4(1)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.1.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun  5 15:55:08 2025
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 10.4(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale a imagem do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

Mostrar exemplo

```
cs2# install all nxos bootflash:nxos.10.4.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.10.4.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image  
bootflash:/nxos.10.4.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image  
bootflash:/nxos.10.4.2.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	10.4 (1)	10.4 (2)
Yes			
1	bios	xx.xx.:xx.xx	xxx
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.

9. Verifique a nova versão do software NX-OS após a reinicialização do switch:

show version

Mostrar exemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, 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 01.14
NXOS: version 10.4(2) [Feature Release]
Host NXOS: version 10.4(2)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.2.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 10.4(2)
```

```
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	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.10.4.2.F.img module all
```

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 de todas as portas no cluster.

a. Portas de cluster

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

ii. Verifique o estado de funcionamento do switch no cluster:

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

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp

node1-01/cdp
      e10a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
      e10b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/3
N9K-C9364D-GX2A
      e11a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
      e11b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/4
N9K-C9364D-GX2A
      e1a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
      e1b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/1
N9K-C9364D-GX2A
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
      e7b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/2
N9K-C9364D-GX2A

node1-02/cdp
      e10a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
      e10b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/3
N9K-C9364D-GX2A
      e11a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
      e11b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/4
N9K-C9364D-GX2A
      e1a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
      e1b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/1
N9K-C9364D-GX2A
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
      e7b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/2
N9K-C9364D-GX2A
      .
```

```

.
.

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                Type                                Address
Model                                -----
-----
cs2 (FDOXXXXXXXXX)                   cluster-network                   10.228.137.233
N9K-C9364D-GX2A
    Serial Number: FDOXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)                   cluster-network                   10.228.137.253
N9K-C9364D-GX2A
    Serial Number: FLMXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

```

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: elb-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)

Node: node1-02
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```



```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.1	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

13. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	false
node1-04	true	true	true

4 entries were displayed.

14. Repita os passos 6 a 13 para instalar o software NX-OS no switch cs1.

15. Ative a reversão automática nos LIFs do cluster.

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

16. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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				
e7a	node1-01_clus1	up/up	169.254.36.44/16	node1-01
	true			
e7b	node1-01_clus2	up/up	169.254.7.5/16	node1-01
	true			
e7a	node1-02_clus1	up/up	169.254.197.206/16	node1-02
	true			
e7b	node1-02_clus2	up/up	169.254.195.186/16	node1-02
	true			
e7a	node1-03_clus1	up/up	169.254.192.49/16	node1-03
	true			
e7b	node1-03_clus2	up/up	169.254.182.76/16	node1-03
	true			
e7a	node1-04_clus1	up/up	169.254.59.49/16	node1-04
	true			
e7b	node1-04_clus2	up/up	169.254.62.244/16	node1-04
	true			

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif-name>
```

O que vem a seguir?

Após instalar ou atualizar o software NX-OS, você [instalar ou atualizar o arquivo de configuração de](#)

[referência \(RCF\)](#)" .

Instale ou atualize o RCF

Visão geral da instalação ou atualização do arquivo de configuração de referência (RCF)

Você instala o RCF após configurar o switch Nexus 9364D-GX2A pela primeira vez. Você atualiza a versão do RCF quando já tiver uma versão existente do arquivo RCF instalada no switch.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configuração RCF disponível

- **Cluster-HA-Storage AFX** - Todas as portas estão configuradas no modo breakout 4x100GbE, que oferece suporte universal a clusters de nós AFX, alta disponibilidade (HA), portas de armazenamento e portas de prateleira de armazenamento NX224. ISL de 400GbE entre switches. (*Cluster-HA-Storage AFX RCF_vxx.x*).

Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de banner e notas importantes no seu RCF. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

Documentação sugerida

- ["Switches Ethernet Cisco \(NSS\)"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 9000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do LIF do cluster são node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 e node1-04_clus2.
- O `cluster1::*>` O prompt indica o nome do cluster.

Consulte o ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

O que vem a seguir?

Depois de revisar o procedimento de instalação do RCF ou atualização do RCF, você ["instalar o RCF"](#) ou ["atualize seu RCF"](#) conforme necessário.

Instale o RCF

Você instala o RCF depois de configurar o switch Nexus 9364D-GX2A pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma conexão de console com o switch. A conexão com o console é opcional se você tiver acesso remoto ao switch.
- Os switches cs1 e cs2 estão ligados e a configuração inicial dos switches está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão desejada do NX-OS foi instalada.
- As conexões ISL entre os switches estão conectadas.
- As portas do cluster de nós ONTAP não estão conectadas.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch cs1 usando SSH ou usando um console serial.
2. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória flash de inicialização no switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9364D-GX2A-RCF-v10.0-Shared.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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o arquivo RCF. NX9364D-GX2A-RCF-v10.0-Shared.txt sendo instalado no switch cs1:

```
cs1# copy NX9364D-GX2A-RCF-v10.0-Shared.txt running-config echo-  
commands
```

4. Examine a saída do banner do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

Mostrar exemplo

```
cs1# show banner motd  
  
*****  
*****  
* NetApp Reference Configuration File (RCF)  
*  
* Switch    : NX9364D-GX2A  
* Filename  : NX9364D-GX2A-RCF-v10.0-Shared.txt  
* Date      : 05-09-2025  
* Version   : v10.0  
* Port Usage:  
* Ports 1-62: 100GbE Intra-Cluster/HA/Storage Ports, int e1/{1-  
62}/1-4  
* Ports 63-64: Intra-Cluster ISL Ports, int e1/63-64  
*  
* IMPORTANT NOTES  
* Interface port-channel999 is reserved to identify the version of  
this file.  
*  
*****  
*****
```

5. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta

- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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

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 1536" >>
bootflash:write_erase.cfg
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

7. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Emita 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
```

9. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Reinicie o switch:


```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

11. Repita os passos 1 a 10 no switch cs2.
12. Conecte as portas de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch conectadas às portas do cluster estão ativas:

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1          eth  trunk  up      none
100G(D) --
Eth1/9/4          1          eth  trunk  up      none
100G(D) --
Eth1/15/1         1          eth  trunk  up      none
100G(D) --
Eth1/15/2         1          eth  trunk  up      none
100G(D) --
Eth1/15/3         1          eth  trunk  up      none
100G(D) --
Eth1/15/4         1          eth  trunk  up      none
100G(D) --
Eth1/16/1         1          eth  trunk  up      none
100G(D) --
Eth1/16/2         1          eth  trunk  up      none
100G(D) --
Eth1/16/3         1          eth  trunk  up      none
100G(D) --
Eth1/16/4         1          eth  trunk  up      none
100G(D) --
Eth1/17/1         1          eth  trunk  up      none
100G(D) --
Eth1/17/2         1          eth  trunk  up      none
100G(D) --
Eth1/17/3         1          eth  trunk  up      none
100G(D) --
Eth1/17/4         1          eth  trunk  up      none
100G(D) --
.
.
```

2. Verifique se os nós do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/63, Eth1/64, Eth1/65, Eth1/66, Eth1/1/1, Eth1/1/2, Eth1/1/3, Eth1/1/4, Eth1/2/1, Eth1/2/2, Eth1/2/3, Eth1/2/4, Eth1/3/1, Eth1/3/2, Eth1/3/3, Eth1/3/4, Eth1/4/1, Eth1/4/2, Eth1/4/3, Eth1/4/4, Eth1/5/1, Eth1/5/2, Eth1/5/3, Eth1/5/4, Eth1/6/1, Eth1/6/2, Eth1/6/3, Eth1/6/4, Eth1/7/1, Eth1/7/2, Eth1/7/3, Eth1/7/4, Eth1/8/1, Eth1/8/2, Eth1/8/3, Eth1/8/4, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4, Eth1/11/1, Eth1/11/2, Eth1/11/3, Eth1/11/4, Eth1/12/1, Eth1/12/2, Eth1/12/3, Eth1/12/4, Eth1/13/1, Eth1/13/2, Eth1/13/3, Eth1/13/4, Eth1/14/1,

Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2

Eth1/15/4, Eth1/16/1

Eth1/16/3, Eth1/16/4

Eth1/17/2, Eth1/17/3

Eth1/18/1, Eth1/18/2

Eth1/18/4, Eth1/19/1

Eth1/19/3, Eth1/19/4

Eth1/20/2, Eth1/20/3

Eth1/21/1, Eth1/21/2

Eth1/21/4, Eth1/22/1

Eth1/22/3, Eth1/22/4

Eth1/23/2, Eth1/23/3

Eth1/24/1, Eth1/24/2

Eth1/24/4, Eth1/25/1

Eth1/25/3, Eth1/25/4

Eth1/26/2, Eth1/26/3

Eth1/27/1, Eth1/27/2

Eth1/27/4, Eth1/28/1

Eth1/28/3, Eth1/28/4

Eth1/29/2, Eth1/29/3

Eth1/30/1, Eth1/30/2

Eth1/30/4, Eth1/31/1

Eth1/14/4,

Eth1/15/3,

Eth1/16/2,

Eth1/17/1,

Eth1/17/4,

Eth1/18/3,

Eth1/19/2,

Eth1/20/1,

Eth1/20/4,

Eth1/21/3,

Eth1/22/2,

Eth1/23/1,

Eth1/23/4,

Eth1/24/3,

Eth1/25/2,

Eth1/26/1,

Eth1/26/4,

Eth1/27/3,

Eth1/28/2,

Eth1/29/1,

Eth1/29/4,

Eth1/30/3,

Eth1/31/2,

Eth1/31/3, Eth1/31/4

Eth1/32/2, Eth1/32/3

Eth1/33/1, Eth1/33/2

Eth1/33/4, Eth1/34/1

Eth1/34/3, Eth1/34/4

Eth1/35/2, Eth1/35/3

Eth1/36/1, Eth1/36/2

Eth1/36/4, Eth1/37/1

Eth1/37/3, Eth1/37/4

Eth1/38/2, Eth1/38/3

Eth1/39/1, Eth1/39/2

Eth1/39/4, Eth1/40/1

Eth1/40/3, Eth1/40/4

Eth1/41/2, Eth1/41/3

Eth1/42/1, Eth1/42/2

Eth1/42/4, Eth1/43/1

Eth1/43/3, Eth1/43/4

Eth1/44/2, Eth1/44/3

Eth1/45/1, Eth1/45/2

Eth1/45/4, Eth1/46/1

Eth1/46/3, Eth1/46/4

Eth1/47/2, Eth1/47/3

Eth1/48/1, Eth1/48/2

Eth1/32/1,

Eth1/32/4,

Eth1/33/3,

Eth1/34/2,

Eth1/35/1,

Eth1/35/4,

Eth1/36/3,

Eth1/37/2,

Eth1/38/1,

Eth1/38/4,

Eth1/39/3,

Eth1/40/2,

Eth1/41/1,

Eth1/41/4,

Eth1/42/3,

Eth1/43/2,

Eth1/44/1,

Eth1/44/4,

Eth1/45/3,

Eth1/46/2,

Eth1/47/1,

Eth1/47/4,

Eth1/48/3,

Eth1/48/4, Eth1/49/1		Eth1/49/2,
Eth1/49/3, Eth1/49/4		Eth1/50/1,
Eth1/50/2, Eth1/50/3		Eth1/50/4,
Eth1/51/1, Eth1/51/2		Eth1/51/3,
Eth1/51/4, Eth1/52/1		Eth1/52/2,
Eth1/52/3, Eth1/52/4		Eth1/53/1,
Eth1/53/2, Eth1/53/3		Eth1/53/4,
Eth1/54/1, Eth1/54/2		Eth1/54/3,
Eth1/54/4, Eth1/55/1		Eth1/55/2,
Eth1/55/3, Eth1/55/4		Eth1/56/1,
Eth1/56/2, Eth1/56/3		Eth1/56/4,
Eth1/57/1, Eth1/57/2		Eth1/57/3,
Eth1/57/4, Eth1/58/1		Eth1/58/2,
Eth1/58/3, Eth1/58/4		Eth1/59/1,
Eth1/59/2, Eth1/59/3		Eth1/59/4,
Eth1/60/1, Eth1/60/2		Eth1/60/3,
Eth1/60/4, Eth1/61/1		Eth1/61/2,
Eth1/61/3, Eth1/61/4		Eth1/62/1,
Eth1/62/2, Eth1/62/3		Eth1/62/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		

Eth1/4/3	Eth1/4/1, Eth1/4/2,
Eth1/5/2	Eth1/4/4, Eth1/5/1,
Eth1/6/1	Eth1/5/3, Eth1/5/4,
Eth1/6/4	Eth1/6/2, Eth1/6/3,
Eth1/7/3	Eth1/7/1, Eth1/7/2,
Eth1/8/2	Eth1/7/4, Eth1/8/1,
Eth1/9/1	Eth1/8/3, Eth1/8/4,
Eth1/9/4	Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3	Eth1/10/1,
Eth1/11/1, Eth1/11/2	Eth1/10/4,
Eth1/11/4, Eth1/12/1	Eth1/11/3,
Eth1/12/3, Eth1/12/4	Eth1/12/2,
Eth1/13/2, Eth1/13/3	Eth1/13/1,
Eth1/14/1, Eth1/14/2	Eth1/13/4,
Eth1/14/4, Eth1/15/1	Eth1/14/3,
Eth1/15/3, Eth1/15/4	Eth1/15/2,
Eth1/16/2, Eth1/16/3	Eth1/16/1,
Eth1/17/1, Eth1/17/2	Eth1/16/4,
Eth1/17/4, Eth1/18/1	Eth1/17/3,
Eth1/18/3, Eth1/18/4	Eth1/18/2,
Eth1/19/2, Eth1/19/3	Eth1/19/1,
Eth1/20/1, Eth1/20/2	Eth1/19/4,
Eth1/20/4, Eth1/21/1	Eth1/20/3,

Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2
Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2

Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,
Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,

Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3
Eth1/53/1, Eth1/53/2
Eth1/53/4, Eth1/54/1
Eth1/54/3, Eth1/54/4
Eth1/55/2, Eth1/55/3

Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,
Eth1/52/4,
Eth1/53/3,
Eth1/54/2,
Eth1/55/1,

Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
18 VLAN0018	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
Eth1/8/2		Eth1/7/4, Eth1/8/1,
Eth1/9/1		Eth1/8/3, Eth1/8/4,
Eth1/9/4		Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3		Eth1/10/1,
		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/59/4, Eth1/60/1

Eth1/60/3, Eth1/60/4

Eth1/61/2, Eth1/61/3

Eth1/62/1, Eth1/62/2

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/60/2,

Eth1/61/1,

Eth1/61/4,

Eth1/62/3, Eth1/62/4

30	VLAN0030	active	Eth1/1/1, Eth1/1/2,
	Eth1/1/3		Eth1/1/4, Eth1/2/1,
	Eth1/2/2		Eth1/2/3, Eth1/2/4,
	Eth1/3/1		Eth1/3/2, Eth1/3/3,
	Eth1/3/4		Eth1/4/1, Eth1/4/2,
	Eth1/4/3		Eth1/4/4, Eth1/5/1,
	Eth1/5/2		Eth1/5/3, Eth1/5/4,
	Eth1/6/1		Eth1/6/2, Eth1/6/3,
	Eth1/6/4		Eth1/7/1, Eth1/7/2,
	Eth1/7/3		Eth1/7/4, Eth1/8/1,
	Eth1/8/2		Eth1/8/3, Eth1/8/4,
	Eth1/9/1		Eth1/9/2, Eth1/9/3,
	Eth1/9/4		Eth1/10/1,
	Eth1/10/2, Eth1/10/3		Eth1/10/4,
	Eth1/11/1, Eth1/11/2		Eth1/11/3,
	Eth1/11/4, Eth1/12/1		Eth1/12/2,
	Eth1/12/3, Eth1/12/4		Eth1/13/1,
	Eth1/13/2, Eth1/13/3		Eth1/13/4,
	Eth1/14/1, Eth1/14/2		Eth1/14/3,
	Eth1/14/4, Eth1/15/1		Eth1/15/2,
	Eth1/15/3, Eth1/15/4		Eth1/16/1,
	Eth1/16/2, Eth1/16/3		Eth1/16/4,
	Eth1/17/1, Eth1/17/2		Eth1/17/3,
	Eth1/17/4, Eth1/18/1		

Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2

Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,

Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2
Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3

Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,
Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,

Eth1/53/1, Eth1/53/2		Eth1/52/4,
Eth1/53/4, Eth1/54/1		Eth1/53/3,
Eth1/54/3, Eth1/54/4		Eth1/54/2,
Eth1/55/2, Eth1/55/3		Eth1/55/1,
Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
40 VLAN0040	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
		Eth1/7/4, Eth1/8/1,

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/59/4, Eth1/60/1

Eth1/60/2,

Eth1/60/3, Eth1/60/4

Eth1/61/1,

Eth1/61/2, Eth1/61/3

Eth1/61/4,

Eth1/62/1, Eth1/62/2

Eth1/62/3, Eth1/62/4

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/62/2	none		
Eth1/62/3	none		
Eth1/62/4	none		
Eth1/63	none		
Eth1/64	none		
Pol	1		



Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

3. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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      Eth1/63 (P)  Eth1/64 (P)
999    Po999 (SD)    Eth      NONE      --
cs1#
```

Etapa 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager oferece um fluxo de trabalho simples e fácil para a configuração e instalação de clusters, incluindo a atribuição de um endereço IP de gerenciamento de nó, a inicialização do cluster, a criação de uma camada local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Vá para ["Configurar o ONTAP em um novo cluster com o System Manager"](#) Para obter instruções de configuração.

O que vem a seguir?

Depois de instalar o RCF, você ["verificar a configuração SSH"](#).

Atualize sua versão do RCF

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapa 1: Prepare-se para a atualização

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exiba as portas do cluster em cada nó que estão conectadas aos switches:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1-01/cdp
          e10a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3  N9K-
C9364D-GX2A
          e10b   cs1 (FDOXXXXXXXXXX)      Ethernet1/13/3  N9K-
C9364D-GX2A
          e11a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4  N9K-
C9364D-GX2A
          e11b   cs1 (FDOXXXXXXXXXX)      Ethernet1/13/4  N9K-
C9364D-GX2A
          e1a    cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1  N9K-
C9364D-GX2A
          e1b    cs1 (FDOXXXXXXXXXX)      Ethernet1/13/1  N9K-
C9364D-GX2A
          .
          .
          .
          e7a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2  N9K-
C9364D-GX2A
          e7b   cs1 (FDOXXXXXXXXXX)      Ethernet1/13/2  N9K-
C9364D-GX2A
node1-01/lldp
          e10a   cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/3  -
          e10b   cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/3  -
          e11a   cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/4  -
          e11b   cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/4  -
          e1a    cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/1  -
          e1b    cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/1  -
          .
          .
          .
          e7a   cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/2  -
          e7b   cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/2  -
          .
          .
          .
```


4. Verifique o status administrativo e operacional de cada porto.

a. **Portas de cluster**

i. Verifique se todas as portas do cluster estão ativas e com status íntegro:

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

Mostrar exemplo

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

Node: node1-01

Ignore

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node1-02

Ignore

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node1-03

Ignore

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

cluster1::*>

ii. Verifique se todas as interfaces de cluster (LIFs) estão na porta principal:

```
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			
	node1-01_clus1	up/up	169.254.3.4/23
node1-01	e7a true		
	node1-01_clus2	up/up	169.254.3.5/23
node1-01	e7b true		
	node1-02_clus1	up/up	169.254.3.8/23
node1-02	e7a true		
	node1-02_clus2	up/up	169.254.3.9/23
node1-02	e7b true		
	node1-03_clus1	up/up	169.254.1.3/23
node1-03	e7a true		
	node1-03_clus2	up/up	169.254.1.1/23
node1-03	e7b true		
	node1-04_clus1	up/up	169.254.1.6/23
node1-04	e7a true		
	node1-04_clus2	up/up	169.254.1.7/23
node1-04	e7b true		
8 entries were displayed.			

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

```
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 (FDOXXXXXXXX)                         cluster-network                     10.228.137.233
N9K-C9364D-GX2A
    Serial Number: FDOXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs2 (FLMXXXXXXXX)                         cluster-network                     10.228.137.234
N9K-C9364D-GX2A
    Serial Number: FLMXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP
```

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: elb-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: ela-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```


Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Desativar a reversão automática nas LIFs do cluster:

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

Etapa 2: Configurar portas

1. No switch cs1, desligue as portas conectadas a todas as portas dos nós.

```

cs1# config
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,e1/7/1-4,e1/8/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-
4,e1/14/1-4,e1/15/1-4,e1/16/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-
4,e1/22/1-4,e1/23/1-4,e1/24/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-4,e1/29/1-
4,e1/30/1-4,e1/31/1-4,e1/32/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/33/1-4,e1/34/1-4,e1/35/1-4,e1/36/1-4,e1/37/1-
4,e1/38/1-4,e1/39/1-4,e1/40/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/41/1-4,e1/42/1-4,e1/43/1-4,e1/44/1-4,e1/35/1-
4,e1/46/1-4,e1/47/1-4,e1/48/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/49/1-4,e1/50/1-4,e1/51/1-4,e1/52/1-4,e1/53/1-
4,e1/54/1-4,e1/55/1-4,e1/56/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/57/1-4,e1/58/1-4,e1/59/1-4,e1/60/1-4,e1/61/1-
4,e1/62/1-4
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit

```



Certifique-se de desativar **todas** as portas conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) para obter mais detalhes.

2. Verifique se as LIFs do cluster foram transferidas 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				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			

8 entries were displayed.

3. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

4. Caso ainda não o tenha feito, 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 versões mais recentes, use o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, use uma ferramenta de comparação/diferenciação de terceiros.
5. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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
```

```
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 1536" >>  
bootflash:write_erase.cfg
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

6. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

7. Emita 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
```

8. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

9. Reinicie o switch:

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

10. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

11. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória flash de inicialização no switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9364D-GX2A-RCF-v10.0-Shared.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)...
```

12. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Este exemplo mostra o arquivo RCF. NX9364D-GX2A-RCF-v10.0-Shared.txt sendo instalado no switch cs1:

```
cs1# copy NX9364D-GX2A-RCF-v10.0-Shared.txt running-config echo-commands
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

13. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

14. Reaplique quaisquer personalizações anteriores à configuração do switch.
15. Após verificar se as versões do RCF, as adições personalizadas e as configurações de interruptores estão corretas, copie o arquivo running-config para o arquivo startup-config.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

16. Reinicie o interruptor cs1. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e os eventos de "portas de cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

17. Verifique a integridade das portas no cluster.

a. Portas de cluster

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper

e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

ii. Verifique o estado de saúde do switch no cluster.

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

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


Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FLMXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9364D-GX2A			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/2
N9K-C9364D-GX2A			
node1-02/cdp			
	.		
	.		
	.		

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		

```
10.4(2)
Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)          cluster-network    10.228.137.234
N9K-C9364D-GX2A
  Serial Number: FLMXXXXXXXXX
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
10.4(2)
Version Source: CDP/ISDP

2 entries were displayed.
```

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)

Node: node1-01
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE

cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)

Node: node1-02
Link 0 Status: up
Link 1 Status: up
Is Link 0 Active: true
Is Link 1 Active: true
IC RDMA Connection: up
Slot: 0
Debug Firmware: no

Interconnect Port 0 :
Port Name: e1a-17
MTU: 4096
Link Information: ACTIVE

Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

18. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

19. Repita os passos 4 a 18 no switch cs2.

20. Ativar reversão automática nos LIFs do cluster:

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

Etapa 3: Verifique a configuração de rede do cluster e a integridade do cluster.

1. Verifique se as portas do switch conectadas às portas do cluster estão ativas.

```
show interface brief
```

Mostrar exemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1      eth  trunk  up      none
100G(D) --
Eth1/9/4          1      eth  trunk  up      none
100G(D) --
Eth1/15/1         1      eth  trunk  up      none
100G(D) --
Eth1/15/2         1      eth  trunk  up      none
100G(D) --
Eth1/15/3         1      eth  trunk  up      none
100G(D) --
Eth1/15/4         1      eth  trunk  up      none
100G(D) --
Eth1/16/1         1      eth  trunk  up      none
100G(D) --
Eth1/16/2         1      eth  trunk  up      none
100G(D) --
Eth1/16/3         1      eth  trunk  up      none
100G(D) --
Eth1/16/4         1      eth  trunk  up      none
100G(D) --
Eth1/17/1         1      eth  trunk  up      none
100G(D) --
Eth1/17/2         1      eth  trunk  up      none
100G(D) --
Eth1/17/3         1      eth  trunk  up      none
100G(D) --
Eth1/17/4         1      eth  trunk  up      none
100G(D) --
.
.
.
```

2. Verifique se os nós esperados ainda estão conectados:

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs2 (FDOXXXXXXXXX) Eth1/31	Eth1/63	179	R S I s	N9K-C9332D-GX2B
cs2 (FDOXXXXXXXXX) Eth1/32	Eth1/64	179	R S I s	N9K-C9332D-GX2B
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K
node1-02 e7a	Eth1/9/2	138	H	AFX-1K
node1-02 e10a	Eth1/9/3	138	H	AFX-1K
node1-02 e11a	Eth1/9/4	138	H	AFX-1K
node1-03 e1a	Eth1/15/1	138	H	AFX-1K
node1-03 e7a	Eth1/15/2	138	H	AFX-1K
node1-03 e10a	Eth1/15/3	138	H	AFX-1K
node1-03 e11a	Eth1/15/4	138	H	AFX-1K
node1-04 e1a	Eth1/16/1	173	H	AFX-1K
node1-04 e7a	Eth1/16/2	173	H	AFX-1K
node1-04 e10a	Eth1/16/3	173	H	AFX-1K

```
node1-04          Eth1/16/4      173    H      AFX-1K
e11a
```

```
Total entries displayed: 18
```

3. Verifique se os nós do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/63, Eth1/64 Eth1/65, Eth1/66, Eth1/1/1 Eth1/1/2, Eth1/1/3, Eth1/1/4 Eth1/2/1, Eth1/2/2, Eth1/2/3 Eth1/2/4, Eth1/3/1, Eth1/3/2 Eth1/3/3, Eth1/3/4, Eth1/4/1 Eth1/4/2, Eth1/4/3, Eth1/4/4 Eth1/5/1, Eth1/5/2, Eth1/5/3 Eth1/5/4, Eth1/6/1, Eth1/6/2 Eth1/6/3, Eth1/6/4, Eth1/7/1 Eth1/7/2, Eth1/7/3, Eth1/7/4 Eth1/8/1, Eth1/8/2, Eth1/8/3 Eth1/8/4, Eth1/9/1, Eth1/9/2 Eth1/9/3, Eth1/9/4, Eth1/10/1 Eth1/10/2, Eth1/10/3, Eth1/10/4 Eth1/11/1, Eth1/11/2, Eth1/11/3 Eth1/11/4, Eth1/12/1, Eth1/12/2 Eth1/12/3, Eth1/12/4, Eth1/13/1 Eth1/13/2, Eth1/13/3, Eth1/13/4 Eth1/14/1,

Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2

Eth1/15/4, Eth1/16/1

Eth1/16/3, Eth1/16/4

Eth1/17/2, Eth1/17/3

Eth1/18/1, Eth1/18/2

Eth1/18/4, Eth1/19/1

Eth1/19/3, Eth1/19/4

Eth1/20/2, Eth1/20/3

Eth1/21/1, Eth1/21/2

Eth1/21/4, Eth1/22/1

Eth1/22/3, Eth1/22/4

Eth1/23/2, Eth1/23/3

Eth1/24/1, Eth1/24/2

Eth1/24/4, Eth1/25/1

Eth1/25/3, Eth1/25/4

Eth1/26/2, Eth1/26/3

Eth1/27/1, Eth1/27/2

Eth1/27/4, Eth1/28/1

Eth1/28/3, Eth1/28/4

Eth1/29/2, Eth1/29/3

Eth1/30/1, Eth1/30/2

Eth1/30/4, Eth1/31/1

Eth1/14/4,

Eth1/15/3,

Eth1/16/2,

Eth1/17/1,

Eth1/17/4,

Eth1/18/3,

Eth1/19/2,

Eth1/20/1,

Eth1/20/4,

Eth1/21/3,

Eth1/22/2,

Eth1/23/1,

Eth1/23/4,

Eth1/24/3,

Eth1/25/2,

Eth1/26/1,

Eth1/26/4,

Eth1/27/3,

Eth1/28/2,

Eth1/29/1,

Eth1/29/4,

Eth1/30/3,

Eth1/31/2,

Eth1/31/3, Eth1/31/4

Eth1/32/2, Eth1/32/3

Eth1/33/1, Eth1/33/2

Eth1/33/4, Eth1/34/1

Eth1/34/3, Eth1/34/4

Eth1/35/2, Eth1/35/3

Eth1/36/1, Eth1/36/2

Eth1/36/4, Eth1/37/1

Eth1/37/3, Eth1/37/4

Eth1/38/2, Eth1/38/3

Eth1/39/1, Eth1/39/2

Eth1/39/4, Eth1/40/1

Eth1/40/3, Eth1/40/4

Eth1/41/2, Eth1/41/3

Eth1/42/1, Eth1/42/2

Eth1/42/4, Eth1/43/1

Eth1/43/3, Eth1/43/4

Eth1/44/2, Eth1/44/3

Eth1/45/1, Eth1/45/2

Eth1/45/4, Eth1/46/1

Eth1/46/3, Eth1/46/4

Eth1/47/2, Eth1/47/3

Eth1/48/1, Eth1/48/2

Eth1/32/1,

Eth1/32/4,

Eth1/33/3,

Eth1/34/2,

Eth1/35/1,

Eth1/35/4,

Eth1/36/3,

Eth1/37/2,

Eth1/38/1,

Eth1/38/4,

Eth1/39/3,

Eth1/40/2,

Eth1/41/1,

Eth1/41/4,

Eth1/42/3,

Eth1/43/2,

Eth1/44/1,

Eth1/44/4,

Eth1/45/3,

Eth1/46/2,

Eth1/47/1,

Eth1/47/4,

Eth1/48/3,

Eth1/48/4, Eth1/49/1		Eth1/49/2,
Eth1/49/3, Eth1/49/4		Eth1/50/1,
Eth1/50/2, Eth1/50/3		Eth1/50/4,
Eth1/51/1, Eth1/51/2		Eth1/51/3,
Eth1/51/4, Eth1/52/1		Eth1/52/2,
Eth1/52/3, Eth1/52/4		Eth1/53/1,
Eth1/53/2, Eth1/53/3		Eth1/53/4,
Eth1/54/1, Eth1/54/2		Eth1/54/3,
Eth1/54/4, Eth1/55/1		Eth1/55/2,
Eth1/55/3, Eth1/55/4		Eth1/56/1,
Eth1/56/2, Eth1/56/3		Eth1/56/4,
Eth1/57/1, Eth1/57/2		Eth1/57/3,
Eth1/57/4, Eth1/58/1		Eth1/58/2,
Eth1/58/3, Eth1/58/4		Eth1/59/1,
Eth1/59/2, Eth1/59/3		Eth1/59/4,
Eth1/60/1, Eth1/60/2		Eth1/60/3,
Eth1/60/4, Eth1/61/1		Eth1/61/2,
Eth1/61/3, Eth1/61/4		Eth1/62/1,
Eth1/62/2, Eth1/62/3		Eth1/62/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		

Eth1/4/3

Eth1/5/2

Eth1/6/1

Eth1/6/4

Eth1/7/3

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/4/1, Eth1/4/2,

Eth1/4/4, Eth1/5/1,

Eth1/5/3, Eth1/5/4,

Eth1/6/2, Eth1/6/3,

Eth1/7/1, Eth1/7/2,

Eth1/7/4, Eth1/8/1,

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2
Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2

Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,
Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,

Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3
Eth1/53/1, Eth1/53/2
Eth1/53/4, Eth1/54/1
Eth1/54/3, Eth1/54/4
Eth1/55/2, Eth1/55/3

Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,
Eth1/52/4,
Eth1/53/3,
Eth1/54/2,
Eth1/55/1,

Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
18 VLAN0018	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
Eth1/8/2		Eth1/7/4, Eth1/8/1,
Eth1/9/1		Eth1/8/3, Eth1/8/4,
Eth1/9/4		Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3		Eth1/10/1,
		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/59/4, Eth1/60/1

Eth1/60/3, Eth1/60/4

Eth1/61/2, Eth1/61/3

Eth1/62/1, Eth1/62/2

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/60/2,

Eth1/61/1,

Eth1/61/4,

Eth1/62/3, Eth1/62/4

30	VLAN0030	active	Eth1/1/1, Eth1/1/2,
	Eth1/1/3		Eth1/1/4, Eth1/2/1,
	Eth1/2/2		Eth1/2/3, Eth1/2/4,
	Eth1/3/1		Eth1/3/2, Eth1/3/3,
	Eth1/3/4		Eth1/4/1, Eth1/4/2,
	Eth1/4/3		Eth1/4/4, Eth1/5/1,
	Eth1/5/2		Eth1/5/3, Eth1/5/4,
	Eth1/6/1		Eth1/6/2, Eth1/6/3,
	Eth1/6/4		Eth1/7/1, Eth1/7/2,
	Eth1/7/3		Eth1/7/4, Eth1/8/1,
	Eth1/8/2		Eth1/8/3, Eth1/8/4,
	Eth1/9/1		Eth1/9/2, Eth1/9/3,
	Eth1/9/4		Eth1/10/1,
	Eth1/10/2, Eth1/10/3		Eth1/10/4,
	Eth1/11/1, Eth1/11/2		Eth1/11/3,
	Eth1/11/4, Eth1/12/1		Eth1/12/2,
	Eth1/12/3, Eth1/12/4		Eth1/13/1,
	Eth1/13/2, Eth1/13/3		Eth1/13/4,
	Eth1/14/1, Eth1/14/2		Eth1/14/3,
	Eth1/14/4, Eth1/15/1		Eth1/15/2,
	Eth1/15/3, Eth1/15/4		Eth1/16/1,
	Eth1/16/2, Eth1/16/3		Eth1/16/4,
	Eth1/17/1, Eth1/17/2		Eth1/17/3,
	Eth1/17/4, Eth1/18/1		

Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2

Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,

Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2
Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3

Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,
Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,

Eth1/53/1, Eth1/53/2		Eth1/52/4,
Eth1/53/4, Eth1/54/1		Eth1/53/3,
Eth1/54/3, Eth1/54/4		Eth1/54/2,
Eth1/55/2, Eth1/55/3		Eth1/55/1,
Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
40 VLAN0040	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
		Eth1/7/4, Eth1/8/1,

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/59/4, Eth1/60/1

Eth1/60/2,

Eth1/60/3, Eth1/60/4

Eth1/61/1,

Eth1/61/2, Eth1/61/3

Eth1/61/4,

Eth1/62/1, Eth1/62/2

Eth1/62/3, Eth1/62/4

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/62/2	none		
Eth1/62/3	none		
Eth1/62/4	none		
Eth1/63	none		
Eth1/64	none		
Pol	1		



Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

4. Verifique se a ISL entre cs1 e cs2 está funcionando:

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       Eth1/63 (P)      Eth1/64 (P)
999    Po999 (SD)     Eth       NONE       --
```

```
cs1#
```

5. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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					
01	e7a	node1-01_clus1	up/up	169.254.36.44/16	node1-
		true			
		node1-01_clus2	up/up	169.254.7.5/16	node1-
01	e7b	true			
		node1-02_clus1	up/up	169.254.197.206/16	node1-
02	e7a	true			
		node1-02_clus2	up/up	169.254.195.186/16	node1-
02	e7b	true			
		node1-03_clus1	up/up	169.254.192.49/16	node1-
03	e7a	true			
		node1-03_clus2	up/up	169.254.182.76/16	node1-
03	e7b	true			
		node1-04_clus1	up/up	169.254.59.49/16	node1-
04	e7a	true			
		node1-04_clus2	up/up	169.254.62.244/16	node1-
04	e7b	true			

8 entries were displayed.

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver vservice_name -lif <lif-name>
```

6. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

7. Verifique a conectividade das interfaces do cluster remoto:

- a. Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet	Source	Destination
Node Date	LIF	LIF
Loss		

node1-01		
6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none		
6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none		
node1-02		
6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none		
6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none		
.		
.		
.		

- b. Alternativamente, você pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
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 vem a seguir?

Depois de atualizar seu RCF, você [verificar a configuração SSH](#) .

Verifique sua configuração SSH.

Se você estiver usando o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches.

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:Thu May 15 15:09:55 2025
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQgQDCQJPZk7OGhg0j1t0NWKylNl8R8zDpuMpU6KKA  
jPOCShTFpibeYQqxOPTCAKACkut8dduZmc3bY9DIOle0cKYQ8PgS2mG9ovQ0RJ56RUNh  
VNPdJuhXM4ckHoiVJxIAbHkbcw8rzawbkT6cNBUiZY3MrOMh0e0CnMRhh9we  
MOo/vQ==
```

```
bitcount:1024
```

```
fingerprint:
```

```
SHA256:TMUXFgyRC3EcIZEVbQ/P0elDByBCJizPJ1XKMkIXfPI
```

```
could not retrieve dsa key information
```

```
ecdsa Keys generated:Thu May 15 15:12:09 2025
```

```
ecdsa-sha2-nistp521
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIAbm1zdHA1MjEAAACFBADquZcNSDA/eLAa  
ItXyxVZxsSJSSE3u4et9B6+RLq162zTe/3A6JTCyBrkfrMhQt9QMQ7XrMqJGxLSinXhyU  
ClBxwQD/ZbkZueZHiFuYg5hKN97wUYvts+EwpG2mSVonxKKp  
atmtgu48BqKfZTc4LZYL5vgdh5uuktJ0Z8mYHt3xKPXsvw==
```

```
bitcount:521
```

```
fingerprint:
```

```
SHA256:K8LDx6L7sJjLFn8iubUhjt66uk8TYmXwnQKWVD04C1o
```

```
**
```

```
(switch)# show feature | include scpServer
```

```
scpServer          1          enabled
```

```
(switch)# show feature | include ssh
```

```
sshServer          1          enabled
```

```
(switch)#
```

O que vem a seguir?

Após verificar sua configuração SSH, você "[configurar monitoramento de integridade do switch](#)".

Redefinir o switch 9364D-GX2A para os padrões de fábrica

Para redefinir o switch 9364D-GX2A para os padrões de fábrica, você deve apagar as configurações do switch 9364D-GX2A.

Sobre esta tarefa

- Você precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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 um switch Cisco Nexus 9364D-GX2A

Siga estas etapas para substituir um switch Nexus 9364D-GX2A com defeito em uma rede de cluster. Este é um procedimento não disruptivo (NDU).

Requisitos de revisão

Antes de substituir o interruptor, certifique-se de que:

- Você verificou o número de série do interruptor para garantir que o interruptor correto seja substituído.
- Na infraestrutura de cluster e rede existente:
 - O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
 - Todas as portas do cluster estão ativas.

- Todas as interfaces lógicas do cluster (LIFs) estão ativas e em suas portas de origem.
- O ONTAP `cluster ping-cluster -node <node-name>` O comando deve indicar que a conectividade básica e a comunicação com dispositivos maiores que PMTU estão funcionando corretamente em todos os caminhos.
- No switch de substituição Nexus 9364D-GX2A:
 - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - As conexões do nó são as portas 1/1 a 1/62.
 - Todas as portas Inter-Switch Link (ISL) estão desabilitadas nas portas 1/63 e 1/64.
 - O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional NX-OS são carregados no switch.
 - A personalização inicial do interruptor está concluída, conforme detalhado em ["Configurar o switch de cluster 9364D-GX2A"](#).

Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, são copiadas para o novo switch.
- Você executou o comando para migrar uma LIF de cluster do nó onde a LIF de cluster está hospedada.

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos switches Nexus 9364D-GX2A existentes são cs1 e cs2.
- O nome do novo switch Nexus 9364D-GX2A é newcs2.
- Os nomes dos nós são node1-01, node1-02, node1-03 e node1-04.
- Os nomes do cluster LIF são node1-01_clus1 e node1-01_clus2 para node1-01, node1-02_clus1 e node1-02_clus2 para node1-02, node1-03_clus1 e node1-03_clus2 para node1-03 e node1-04_clus1 e node1-04_clus2 para node1-04.
- O prompt para alterações em todos os nós do cluster é `cluster1::*>`

Sobre esta tarefa

O procedimento a seguir baseia-se na seguinte topologia de rede em cluster:

Mostrar exemplo

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

Node: nodel-01

Ignore						
						Speed(Mbps) Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper Status
Status						

e7a	Cluster	Cluster		up	9000	auto/10000 healthy
false						
e7b	Cluster	Cluster		up	9000	auto/10000 healthy
false						

Node: nodel-02

Ignore						
						Speed(Mbps) Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper Status
Status						

e7a	Cluster	Cluster		up	9000	auto/10000 healthy
false						
e7b	Cluster	Cluster		up	9000	auto/10000 healthy
false						

Node: nodel-03

Ignore						
						Speed(Mbps) Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper Status
Status						

e7a	Cluster	Cluster		up	9000	auto/10000 healthy
false						
e7b	Cluster	Cluster		up	9000	auto/10000 healthy
false						

Node: node1-04

Ignore

					Speed(Mbps)	Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status
-----	-----	-----	-----	-----	-----	-----

e7a	Cluster	Cluster		up	9000	auto/10000
false						healthy
e7b	Cluster	Cluster		up	9000	auto/10000
false						healthy

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----

Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7b	true			
.				
.				
.				

cluster1::*> **network device-discovery show -protocol cdp**

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
-----	-----	-----	-----	-----

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-

```

C9364D-GX2A
    e11b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/4    N9K-
C9364D-GX2A
    e1a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/1    N9K-
C9364D-GX2A
    e1b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/1    N9K-
C9364D-GX2A
    .
    .
    .
    e7a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/2    N9K-
C9364D-GX2A
    e7b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/2    N9K-
C9364D-GX2A
    .
    .
    .

```

```
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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
Device-ID	Local Intrfce	Hldtme	Capability	Platform	
Port ID					
newcs2 (FDOXXXXXXXXX)	Eth1/63	179	R S I s	N9K-C9332D-GX2B	
Eth1/31					
newcs2 (FDOXXXXXXXXX)	Eth1/64	179	R S I s	N9K-C9332D-GX2B	
Eth1/32					
node1-01	Eth1/4/1	123	H	AFX-1K	
e1a					
node1-01	Eth1/4/2	123	H	AFX-1K	
e7a					
node1-01	Eth1/4/3	123	H	AFX-1K	
e10a					
node1-01	Eth1/4/4	123	H	AFX-1K	
e11a					
node1-02	Eth1/9/1	138	H	AFX-1K	
e1a					
node1-02	Eth1/9/2	138	H	AFX-1K	
e7a					
node1-02	Eth1/9/3	138	H	AFX-1K	


```

e10a
node1-02          Eth1/9/4          138    H          AFX-1K
e11a
node1-03          Eth1/15/1         138    H          AFX-1K
e1a
node1-03          Eth1/15/2         138    H          AFX-1K
e7a
node1-03          Eth1/15/3         138    H          AFX-1K
e10a
node1-03          Eth1/15/4         138    H          AFX-1K
e11a
node1-04          Eth1/16/1         173    H          AFX-1K
e1a
node1-04          Eth1/16/2         173    H          AFX-1K
e7a
node1-04          Eth1/16/3         173    H          AFX-1K
e10a
node1-04          Eth1/16/4         173    H          AFX-1K
e11a

```

Total entries displayed: 18

newcs2# **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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs1(FDOXXXXXXXXX) Eth1/31	Eth1/63	179	R S I s	N9K-C9332D-GX2B
cs1(FDOXXXXXXXXX) Eth1/32	Eth1/64	179	R S I s	N9K-C9332D-GX2B
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K

node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

Etapa 1: Prepare-se para a substituição

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

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Instale o RCF e a imagem apropriados no switch, newcs2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e NX-OS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e NX-OS, continue para a etapa 2.

- a. Acesse a página *NetApp Cluster and Management Network Switches Reference Configuration File Description* no site de suporte da NetApp .

- b. Clique no link para a *Matriz de Compatibilidade de Rede de Cluster e Rede de Gerenciamento* e, em seguida, observe a versão de software do switch necessária.
 - c. Clique na seta "Voltar" do seu navegador para retornar à página de Descrição, clique em **CONTINUAR**, aceite o contrato de licença e, em seguida, acesse a página de Download.
 - d. Siga os passos na página de Download para baixar os arquivos RCF e NX-OS corretos para a versão do software ONTAP que você está instalando.
3. No novo switch, efetue login como administrador e desligue todas as portas que serão conectadas às interfaces do cluster de nós (portas 1/1 a 1/64).

Se o interruptor que você está substituindo não estiver funcionando e estiver desligado, vá para a Etapa 4. As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em cada nó.

Mostrar exemplo

```
newcs2# config
newcs2(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,e1/7/1-4,e1/8/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-
4,e1/13/1-4,e1/14/1-4,e1/15/1-4,e1/16/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-
4,e1/21/1-4,e1/22/1-4,e1/23/1-4,e1/24/1-4
csnewcs21(config-if-range)# shutdown
newcs2(config)# interface e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-
4,e1/29/1-4,e1/30/1-4,e1/31/1-4,e1/32/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/33/1-4,e1/34/1-4,e1/35/1-4,e1/36/1-
4,e1/37/1-4,e1/38/1-4,e1/39/1-4,e1/40/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/41/1-4,e1/42/1-4,e1/43/1-4,e1/44/1-
4,e1/35/1-4,e1/46/1-4,e1/47/1-4,e1/48/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/49/1-4,e1/50/1-4,e1/51/1-4,e1/52/1-
4,e1/53/1-4,e1/54/1-4,e1/55/1-4,e1/56/1-4
newcs2(config-if-range)# shutdown\
newcs2(config)# interface e1/57/1-4,e1/58/1-4,e1/59/1-4,e1/60/1-
4,e1/61/1-4,e1/62/1-4
newcs2(config-if-range)# shutdown
newcs2(config-if-range)# exit
newcs2(config)# exit
```

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
```

Vserver	Logical Interface	Auto-revert
Cluster	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

```
8 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

- Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, você também pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
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 1/63 e 1/64 no switch Nexus 9364D-GX2A cs1.

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/63-64
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
```

2. Remova todos os cabos do switch Nexus 9364D-GX2B cs2 e conecte-os às mesmas portas no switch Nexus 9364D-GX2A newcs2.
3. Abra as portas ISLs 1/63 e 1/64 entre os switches cs1 e newcs2 e, em seguida, verifique o status da operação do canal da porta.

Port-Channel deve indicar Po1(SU) e Member Ports deve indicar Eth1/63(P) e Eth1/64(P).

Mostrar exemplo

Este exemplo habilita as portas ISL 1/63 e 1/64 e exibe o resumo do canal de porta no switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/63-64
cs1(config-if-range)# no shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
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
-----
-----
11      Po1 (SU)      Eth      LACP      Eth1/63 (P)  Eth1/64 (P)
999     Po999 (SD)    Eth      NONE      --
```

4. Verifique se a porta e7b está ativa em todos os nós:

```
network port show ipspace Cluster
```

Mostrar exemplo

O resultado deverá ser semelhante ao seguinte:

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

Node: node1-01

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-03

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	


```

healthy false
e7b          Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node1-04

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e7a        Cluster      Cluster      up    9000  auto/100000
healthy false
e7b        Cluster      Cluster      up    9000  auto/100000
healthy false

8 entries were displayed.

```

5. No mesmo nó usado na etapa anterior, reverta a LIF do cluster associada à porta da etapa anterior usando o comando `network interface revert`.

Mostrar exemplo

Neste exemplo, o LIF node1-01_clus2 no node1-01 é revertido com sucesso se o valor Home for verdadeiro e a porta for e7b.

Os seguintes comandos retornam LIF node1-01_clus2 sobre node1-01 para o porto de origem e7a e exibe informações sobre os LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se a coluna "Is Home" (É o nó principal) for verdadeira para ambas as interfaces do cluster e elas mostrarem as atribuições de porta corretas, neste exemplo. e7a e e7b no nó 1-01.

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7b	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7a	false			
	.			
	.			
	.			

6. Exibir informações sobre os nós em um cluster:

```
cluster show
```

Mostrar exemplo

Este exemplo mostra que o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1-01	false	true
node1-02	true	true
node1-03	true	true
node1-04	true	true

7. Verifique se todas as portas físicas do cluster estão ativas:

```
network port show ipspace Cluster
```

Mostrar exemplo

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

Node: node1-01

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

.
. .
. .

8. Verifique a conectividade das interfaces do cluster remoto:

- Você pode usar o `network interface check cluster-connectivity show` Comando para exibir os detalhes de uma verificação de acessibilidade para conectividade de cluster:

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

Mostrar exemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, você também pode usar o `cluster ping-cluster -node <node-name>` comando para verificar a conectividade:

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

Mostrar exemplo

```
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. Verifique a integridade de todas as portas no cluster.

a. Portas de cluster

- i. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

```
network port show ipspace Cluster
```

```
network interface show -vserver cluster
```

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

```
show cdp neighbors
```

Mostrar exemplo

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

```
Node: node1-01
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-02
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-03
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper

e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

cluster1::*> **network interface show -vserver cluster**

	Logical	Status	Network	
Current	Current	Is		
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
01	node1-01_clus1	up/up	169.254.209.69/16	node1-
	e7a	true		
01	node1-01_clus2	up/up	169.254.49.125/16	node1-
	e7b	true		
02	node1-02_clus1	up/up	169.254.47.194/16	node1-
	e7b	true		
02	node1-02_clus2	up/up	169.254.19.183/16	node1-
	e7a	false		
	.			
	.			
	.			

cluster1::> **network device-discovery show -protocol cdp**

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			

node1-01/cdp			

```

          e10a    cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
          e10b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
          e11a    cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
          e11b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
          e1a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
          e1b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
          .
          .
          .
          e7a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
          e7b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
          .
          .
          .

```

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			
newcs2 (FDOXXXXXXXXX)	Eth1/63	179	R S I s	N9K-
C9332D-GX2B	Eth1/31			
newcs2 (FDOXXXXXXXXX)	Eth1/64	179	R S I s	N9K-
C9332D-GX2B	Eth1/32			
node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K
e7a				
node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				

node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

newcs2# **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 (FDOXXXXXXXXX)	Eth1/63	179	R S I s	N9K-
C9332D-GX2B	Eth1/31			
cs1 (FDOXXXXXXXXX)	Eth1/64	179	R S I s	N9K-
C9332D-GX2B	Eth1/32			
node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K

```

e7a
node1-01          Eth1/4/3          123      H          AFX-1K
e10a
node1-01          Eth1/4/4          123      H          AFX-1K
e11a
node1-02          Eth1/9/1          138      H          AFX-1K
e1a
node1-02          Eth1/9/2          138      H          AFX-1K
e7a
node1-02          Eth1/9/3          138      H          AFX-1K
e10a
node1-02          Eth1/9/4          138      H          AFX-1K
e11a
node1-03          Eth1/15/1         138      H          AFX-1K
e1a
node1-03          Eth1/15/2         138      H          AFX-1K
e7a
node1-03          Eth1/15/3         138      H          AFX-1K
e10a
node1-03          Eth1/15/4         138      H          AFX-1K
e11a
node1-04          Eth1/16/1         173      H          AFX-1K
e1a
node1-04          Eth1/16/2         173      H          AFX-1K
e7a
node1-04          Eth1/16/3         173      H          AFX-1K
e10a
node1-04          Eth1/16/4         173      H          AFX-1K
e11a

```

Total entries displayed: 18

b. Portas HA

- i. Verifique se todas as portas HA estão ativas e com status íntegro:

```
ha interconnect status show -node <node-name>
```

Mostrar exemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
      Link 0 Status: up
      Link 1 Status: up
    Is Link 0 Active: true
    Is Link 1 Active: true
  IC RDMA Connection: up
        Slot: 0
    Debug Firmware: no
```

```
Interconnect Port 0 :
      Port Name: e1a-17
        MTU: 4096
    Link Information: ACTIVE
```

```
Interconnect Port 1 :
      Port Name: e1b-18
        MTU: 4096
    Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
      Link 0 Status: up
      Link 1 Status: up
    Is Link 0 Active: true
    Is Link 1 Active: true
  IC RDMA Connection: up
        Slot: 0
    Debug Firmware: no
```

```
Interconnect Port 0 :
      Port Name: e1a-17
        MTU: 4096
    Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Portas de armazenamento

- i. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Portas de prateleira de armazenamento

- i. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique o status da conexão de todas as portas da prateleira de armazenamento:

```
storage shelf port show -fields remote-device,remote-  
port,connector-state
```

Mostrar exemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você [configurar monitoramento de integridade do switch](#) .

Comutadores de cluster

BES-53248 com suporte da Broadcom

Começar

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 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 revisar os requisitos de suporte e configuração do EFOS e do ONTAP .

Suporte para EFOS e ONTAP

Consulte a ["Hardware Universe"](#) e a ["matriz de compatibilidade de switches Broadcom"](#) para obter informações sobre a compatibilidade do EFOS e do ONTAP com switches BES-53248. O suporte ao EFOS e ao ONTAP pode variar de acordo com o tipo específico de máquina do switch BES-53248. Para detalhes de todos os tipos de máquina do switch BES-53248, consulte ["Componentes e números de peça para os interruptores do cluster BES-53248"](#). Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#)[^] para obter mais informações sobre os requisitos de instalação do

switch.

Requisitos de configuração

Para configurar um cluster, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para os switches do cluster. Dependendo do tipo de switch de cluster que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído.

Atribuições de portas de comutadores de cluster

Você pode usar a tabela de atribuições de portas do switch de cluster BES-53248, compatível com a Broadcom, como um guia para configurar seu cluster.

Portas de comutação	Utilização de portas
01-16	Nós de porta de cluster 10/25GbE, configuração básica
17-48	Nós de cluster com portas 10/25GbE, com licenças.
49-54	Nós de cluster com portas 40/100GbE, com licenças, adicionados da direita para a esquerda.
55-56	Portas de link entre switches (ISL) de cluster 100GbE, configuração básica

Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Restrição de velocidade do grupo de portas

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

Requisitos adicionais

- Caso adquira licenças adicionais, consulte ["Ativar portas recém-licenciadas"](#) para obter detalhes sobre como ativá-las.
- Se o SSH estiver ativo, você deverá reativá-lo manualmente após executar o comando. `erase startup-config` e reiniciando o switch.

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

Componentes e números de peça para os interruptores do cluster BES-53248

Para instalação e manutenção do switch BES-53248, certifique-se de consultar a lista de

componentes e números de peça.

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



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

Número da peça	Descrição	Versão mínima EFOS	Versão mínima do ONTAP
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = Exaustão do Lado 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, BRDCM SUPP	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Kit de trilhos para montagem em rack Ozeki de 4 postes e 19 polegadas.	N / D	N / D



Observe as seguintes informações referentes aos tipos de máquinas:

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

Você pode determinar o tipo específico da sua máquina 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..... QTCU225xxxxx
```

```
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

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches de cluster BES-53248

Para a instalação 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 Broadcom Support Site: ["Linha de produtos de switches Ethernet da Broadcom"](#).

Título do documento	Descrição
<i>Guia do Administrador EFOS v3.4.3</i>	Fornecer exemplos de como usar o switch BES-53248 em uma rede típica.
<i>Referência de Comandos da CLI do EFOS v3.4.3</i>	Descreve os comandos da interface de linha de comando (CLI) que você usa para visualizar e configurar o software BES-53248.
<i>Guia de Introdução ao EFOS v3.4.3</i>	Fornecer informações detalhadas sobre o switch BES-53248.

Título do documento	Descrição
<i>Guia de Referência SNMP do EFOS v3.4.3</i>	Fornecer exemplos de como usar o switch BES-53248 em uma rede típica.
<i>Parâmetros e valores de escala do EFOS v3.4.3</i>	Descreve os parâmetros de escala padrão com os quais o software EFOS é fornecido e validado nas plataformas suportadas.
<i>Especificações Funcionais do EFOS v3.4.3</i>	Descreve as especificações do software EFOS nas plataformas suportadas.
<i>Notas de lançamento do EFOS v3.4.3</i>	Fornecer informações específicas da versão do software BES-53248.
<i>Matriz de compatibilidade de rede de cluster e rede de gerenciamento</i>	Fornecer informações sobre compatibilidade de rede. A matriz está disponível no site de downloads do switch BES-53248 em " switches de cluster Broadcom ".

Documentação e artigos da base de conhecimento sobre sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos do NetApp Support Site em "[meusuporte.netapp.com](#)" ou do site da Knowledge Base (KB) em "[kb.netapp.com](#)".

Nome	Descrição
" Hardware Universe "	Descreve os requisitos de energia e de instalação para todos os equipamentos NetApp , incluindo gabinetes de sistema, e fornece informações sobre os conectores e opções de cabos relevantes a serem usados, juntamente com seus respectivos números de peça.
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
" ONTAP 9 "	Fornecer informações detalhadas sobre todos os aspectos da versão ONTAP 9.
<i>Como adicionar licenças de porta adicionais para o switch BES-53248 compatível com Broadcom</i>	Fornecer informações detalhadas sobre como adicionar licenças de porta. Consulte este " Artigo da Base de Conhecimento ".

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

"Revisar a cablagem e a configuração."

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

Instale o hardware para o comutador de cluster BES-53248.

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

Passos

1. Analise o ["requisitos de configuração"](#) .
2. Siga as instruções em ["Guia de Instalação do Cluster Switch BES-53248 com suporte da Broadcom"](#) .

O que vem a seguir?

Após instalar o hardware do switch, você pode ["revisar cabeamento e configuração"](#) requisitos.

Análise as considerações sobre cabeamento e configuração.

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

Atribuições de comutador de porta de cluster

Você pode usar a tabela de atribuições de portas do switch de cluster BES-53248, compatível com a Broadcom, como um guia para configurar seu cluster.

Portas de comutação	Utilização de portas
0-16	Nós de porta de cluster 10/25GbE, configuração básica
17-48	Nós de cluster com portas 10/25GbE, com licenças.
49-54	Nós de cluster com portas 40/100GbE, com licenças, adicionados da direita para a esquerda.
55-56	Portas de link entre switches (ISL) de cluster 100GbE, configuração básica

Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch. Consulte o ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Restrição de velocidade do grupo de portas

- Nos switches de cluster BES-53248, as 48 portas 10/25GbE (SFP28/SFP+) são combinadas em 12

grupos de 4 portas, da seguinte forma: Portas 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 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.

Requisitos do FEC

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

Se o lado do controlador estiver `auto` , o lado do switch está configurado para 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 óptica, 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 o FEC da porta 25G para um dos seguintes valores: `auto` ou `fc`, conforme necessário:

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

- Quando definido para `*auto*`:
 - O `auto` A configuração é propagada para o hardware imediatamente e não é necessário reiniciar o sistema.
 - Se `bootarg.cpk_fec_fc_eXx` already exists, ele é apagado do armazenamento de argumentos de inicialização.
 - Após uma reinicialização, o `auto` A configuração permanece em vigor desde `auto` é a configuração FEC padrão.
- Quando definido para `*fc*`:
 - O `FC-FEC` A configuração é propagada para o hardware imediatamente e não é necessário reiniciar.
 - Um novo `bootarg.cpk_fec_fc_eXx` é criado com o valor definido como "verdadeiro".
 - Após uma reinicialização, `FC-FEC` A configuração permanece em vigor para que o código do driver a utilize.

Configurar o software

Fluxograma de instalação de software para switches BES-53248

Para instalar e configurar o software de um switch de cluster BES-53248, siga estes passos:

1

"Configure o interruptor"

Configure o switch de cluster BES-53248.

2

"Instale o software EFOS."

Faça o download e instale o software Ethernet Fabric OS (EFOS) no switch de cluster BES-53248.

3

"Instale as licenças para os switches de cluster BES-53248."

Opcionalmente, adicione novas portas comprando e instalando mais licenças. O modelo básico do switch possui licença para 16 portas 10GbE ou 25GbE e duas portas 100GbE.

4

"Instale o arquivo de configuração de referência (RCF)"

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

5

"Habilite o SSH nos switches de cluster BES-53248."

Se você utiliza o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de coleta de logs, habilite o SSH nos switches.

Configurar o switch de cluster BES-53248

Siga estes passos para realizar a configuração inicial do switch de cluster BES-53248.

Antes de começar

- O hardware está instalado, conforme descrito em ["Instale o hardware"](#).
- Você analisou o seguinte:
 - ["Requisitos de configuração"](#)
 - ["Componentes e números de peça"](#)
 - ["Requisitos de documentação"](#)

Sobre os exemplos

Os exemplos nos procedimentos de configuração utilizam a seguinte nomenclatura de switches e nós:

- Os nomes dos switches NetApp são `cs1` e `cs2`. A atualização começa no segundo switch, `cs2`.
- Os nomes LIF do cluster são `node1_clus1` e `node1_clus2` para o nó 1 e `node2_clus1` e `node2_clus2` para o nó 2.
- O nome do espaço IP é Cluster.

- O `cluster1:` > O prompt indica o nome do cluster.
- As portas do cluster em cada nó são nomeadas `e0a` e `e0b`. Consulte o ["Hardware Universe"](#) para as portas de cluster reais suportadas em sua plataforma.
- Os links entre switches (ISLs) 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 utilizam dois nós, mas você pode ter até 24 nós em um cluster.

Passos

1. Conecte a porta serial a um host ou a uma porta serial.
2. Conecte a porta de gerenciamento (a porta RJ-45 com conector em forma de chave inglesa no lado esquerdo do switch) à mesma rede onde o seu servidor TFTP está localizado.
3. No console, configure as definições seriais do lado do host:
 - 115200 baud
 - 8 bits de dados
 - 1 bit de parada
 - paridade: nenhuma
 - Controle de fluxo: nenhum
4. Faça login no switch como `admin` e pressione **Enter** quando solicitado a inserir uma senha. O nome padrão do switch é **routing**. Quando solicitado, digite `enable`. Isso lhe dá acesso ao modo EXEC privilegiado para configuração do switch.

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

5. Altere o nome do interruptor 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 configurada para usar DHCP por padrão. O endereço IP, a máscara de sub-rede e o endereço do 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 configurada para usar DHCP por padrão. O endereço IP, a máscara de sub-rede e o endereço do gateway padrão são atribuídos automaticamente.

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

1. [[passo 7]]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 versões posteriores

Configure o fuso horário e a sincronização de tempo (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 versões anteriores

Configure o fuso horário e a sincronização de tempo (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. [[passo 10]]Configure a hora manualmente se você não configurou um servidor NTP na etapa anterior.

EFOS 3.10.0.3 e versões posteriores

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 versões 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. [[passo 11]]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 vem a seguir?

Depois de configurar seus switches, você pode ["Instale o software EFOS."](#)

Instale o software EFOS.

Siga estes passos para instalar o software Ethernet Fabric OS (EFOS) no switch de cluster BES-53248.

O software EFOS inclui um conjunto de recursos e protocolos de rede avançados para o desenvolvimento de sistemas de infraestrutura Ethernet e IP. Essa arquitetura de software é adequada para qualquer dispositivo de organização de rede que utilize aplicações que exijam inspeção ou separação minuciosa de pacotes.

Preparar para instalação

Antes de começar

- Este procedimento é adequado apenas para novas instalações.
- Faça o download do software Broadcom EFOS aplicável aos switches do seu cluster a partir do site ["Suporte para switches Ethernet Broadcom"](#) site.
- Garanta o ["O comutador de cluster BES-53248 está configurado."](#) .

Instale o software

Utilize um dos seguintes métodos para instalar o software EFOS:

- [Método 1: Instalar o EFOS](#). Utilizado na maioria dos casos.
- [Método 2: Instalar o EFOS no modo ONIE](#). Utilize esta opção se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS.

Método 1: Instalar o EFOS

Siga os passos abaixo para instalar o software EFOS.

Passos

1. Faça login na porta de console serial do switch ou conecte-se via SSH.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o EFOS, as licenças e o arquivo RCF.

Mostrar exemplo

Este exemplo verifica se o switch está conectado 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. Faça o download do arquivo de imagem para o switch.

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

Protocolo	Pré-requisito
Protocolo de Transferência de Arquivos Trivial (TFTP)	Nenhum
Protocolo de Transferência de Arquivos SSH (SFTP)	Seu pacote de software deve suportar gerenciamento seguro.
FTP	Senha 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 linha de comando são suportadas em plataformas selecionadas quando um utilitário WGET nativo estiver disponível.
HTTPS	Transferências de arquivos baseadas em linha de comando são suportadas em plataformas selecionadas quando um utilitário WGET nativo estiver disponível.

Copiar o arquivo de imagem para a imagem ativa significa que, ao reiniciar, essa imagem estabelecerá a versão do EFOS em execução. A imagem anterior permanece disponível como backup.

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. Exibir as imagens de inicialização para a configuração ativa e de backup:

```
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. Faça login 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 quatro passos para reconfigurar o switch:
 - a. ["Instalar licenças"](#)
 - b. ["Instale o arquivo RCF"](#)
 - c. ["Habilitar SSH"](#)
 - d. ["Configure o monitoramento de integridade do switch."](#)
8. Repita os passos de 1 a 7 no interruptor do parceiro.

Método 2: Instalar o EFOS no modo ONIE

Você pode executar os seguintes passos se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS. Esses passos podem ser usados para instalar a imagem EFOS 3.7.xx, compatível ou não com FIPS, a partir do ONIE, caso o switch não inicialize.

Passos

1. Conecte-se a um console que esteja conectado à porta serial do switch.
2. Inicialize o switch no modo de instalação ONIE.

Durante a inicialização, selecione ONIE quando a mensagem aparecer.

Mostrar exemplo

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

Após selecionar **ONIE**, o interruptor carrega e apresenta várias opções. Selecione **Instalar SO**.

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 inicia no modo de instalação ONIE.

3. Interrompa a descoberta ONIE e configure a interface Ethernet.

Quando a seguinte mensagem aparecer, pressione **Enter** para abrir o console ONIE:

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



A detecção do 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 do 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 switch:

```
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 é instalado e, em seguida, reinicia o switch. Deixe o switch reiniciar normalmente na 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 reinicia sem nenhuma configuração aplicada e retorna às configurações de fábrica. Siga estes cinco passos para reconfigurar o switch:

- "Configurar interruptor"
- "Instalar licenças"
- "Instale o arquivo RCF"
- "Habilitar SSH"

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

9. Repita os passos de 1 a 8 no interruptor do parceiro.

O que vem a seguir

Após instalar o software EFOS, você pode ["Instale suas licenças"](#).

Instale o arquivo de configuração (RCF) e o arquivo de licença

A partir do EFOS 3.12.0.1, é possível instalar o arquivo RCF e o arquivo de licença após configurar o switch 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.

Requisitos de revisão

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 ["Comutadores de cluster Broadcom"](#) página.
- Uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas, necessária caso você esteja instalando apenas o EFOS e mantendo sua versão atual do RCF. Se 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 reinicializações futuras.
- É necessária uma conexão de console com o switch ao instalar o RCF a partir de suas configurações de fábrica. Este requisito é opcional caso você tenha utilizado o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#) para limpar a configuração, previamente.

Documentação sugerida

Consulte a tabela de compatibilidade de switches para as versões suportadas do ONTAP e do RCF. Consulte ["Download do software EFOS"](#). Observe que pode haver dependências de comandos entre a sintaxe de comandos no RCF e a encontrada nas versões do EFOS.

Instale o arquivo de configuração.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do 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::*>` O 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 a ["Hardware Universe"](#) para verificar as portas de cluster corretas em

suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Sobre esta tarefa

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

Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e RCFs, use o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#). Se for necessário apagar completamente as configurações do switch, será preciso realizar a configuração básica novamente. Você deve estar conectado ao switch usando o console serial, pois uma exclusão 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, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

O comando a seguir 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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					
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
```

```
Health      Health      Speed (Mbps)
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 principal:

```
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	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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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. [[passo 6]]Desative a 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 conectadas aos nós do cluster.

```
show isdp neighbor
```

2. No switch de cluster cs2, desligue as portas conectadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conectadas 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 as LIFs do cluster foram migradas 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::*>
```

4. Verifique se o cluster está íntegro:

```
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. Caso ainda não o tenha feito, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração do switch CS2 e execute uma configuração básica.



Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial para apagar as configurações do switch. Este requisito é opcional se você já utilizou o artigo da Base de Conhecimento. ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota?"](#) Para limpar a configuração previamente.



Limpar a configuração não exclui as licenças.

- a. Acesse o switch via SSH.

Prossiga somente quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para ter a configuração apagada.

- b. Entrar no modo privilegiado:

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

- c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior utilizada, alguns comandos podem gerar um erro se uma determinada configuração 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 um reinício do switch:

```
(cs2)# reload
```

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

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

7. Registre todas as personalizações feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, configurar as velocidades das portas ou programar o modo FEC.
8. Copie o arquivo RCF para a memória flash de inicialização do switch cs2 usando um dos seguintes protocolos de transferência: FTP, HTTP, TFTP, SFTP ou SCP.

Este exemplo mostra o uso do HTTP para copiar um arquivo RCF para a memória 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 com o nome de arquivo que você definiu:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
Reference-config.scr 21:54:22	2680	2024 05 31

```
1 configuration script(s) found.
2045 Kbytes free.
```

10. Aplique o script ao interruptor:

```
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 arquivo 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 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 após a aplicação do RCF:

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

Mostrar exemplo

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

LACP	Actor	Admin	Physical	Physical	Link	Link
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 interruptor, verifique se as alterações foram aplicadas:

```
show running-config
```

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

15. Salve a configuração em execução para que ela se torne a configuração de inicialização ao 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, ative as portas conectadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conectadas 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
```

Media	Flow	Link	Physical	Physical	
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 do cluster.

a. Verifique se as portas e0b 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health					Speed (Mbps)
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 o estado de funcionamento do switch 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			
-----	-----	-----	-----
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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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, desligue as portas conectadas às portas de cluster dos nós.

O exemplo a seguir utiliza a saída de exemplo da interface:

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

2. Verifique se as LIFs do cluster foram migradas 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	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 íntegro:

```
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 switch cs1.

5. Ativar reversão automática nos LIFs do cluster:

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

6. Reinicie o interruptor cs1. Isso faz com que as LIFs do cluster voltem às suas portas originais. Você pode ignorar os eventos de "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
(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 conectadas às portas do cluster estão **ativas**:

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

Mostrar exemplo

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

Media	Flow	Link	Physical	Physical	
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 switches cs1 e cs2 está funcionando corretamente:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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	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 íntegro:

```
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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 administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Após instalar o RCF e o arquivo de licença, você pode ["habilitar SSH"](#).

Instale as licenças para os switches de cluster BES-53248.

O modelo básico do switch de cluster BES-53248 possui licença para 16 portas 10GbE ou 25GbE e duas portas 100GbE. Você pode adicionar novas portas adquirindo mais licenças.



Para o EFOS 3.12 e versões posteriores, siga os passos de instalação em ["Instale o arquivo de configuração de referência \(RCF\) e o arquivo de licença."](#) .

Analise 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 + 2PT-40G100G, X190005/R	EFOS 3.4.4.6 e versões posteriores
SW-BES-53248A2-8P-1025G	Chave de licença Broadcom 8 portas 10G25G, X190005/R	EFOS 3.4.4.6 e versões posteriores
SW-BES53248A2-6P-40-100G	Chave de licença Broadcom 6 portas 40G100G, X190005/R	EFOS 3.4.4.6 e versões posteriores



Para resgatar uma chave de transação para um arquivo de chave da licença de porta, consulte ["Portal de Licenças para Switches Ethernet Compatíveis com Broadcom"](#). Consulte o artigo da Knowledge Base ["Como adicionar licenças de porta adicionais para o switch Broadcom BES-53248"](#) para mais detalhes.

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 versões posteriores

Tipo de licença	Detalhes da licença	Versão de firmware suportada
SW-BES-53248A1-G1-16P-LIC	Chave de licença Broadcom 16P 10-25,4P40-100, X190005/R	EFOS 3.4.3.3 e versões posteriores
SW-BES-53248A1-G1-24P-LIC	Chave de licença Broadcom 24P 10-25,6P40-100, X190005/R	EFOS 3.4.3.3 e versões posteriores
SW-BES54248-40-100G-LIC	Chave de licença Broadcom 6Port 40G100G, X190005/R	EFOS 3.4.4.6 e versões posteriores
SW-BES53248-8P-10G25G-LIC	Chave de licença Broadcom 8 portas 10G25G, X190005/R	EFOS 3.4.4.6 e versões posteriores
SW-BES53248-16P-1025G-LIC	Chave de licença Broadcom 16 portas 10G25G, X190005/R	EFOS 3.4.4.6 e versões posteriores
SW-BES53248-24P-1025G-LIC	Chave de licença Broadcom 24 portas 10G25G, X190005/R	EFOS 3.4.4.6 e versões posteriores



Não é necessária uma licença para a configuração básica.

Instalar arquivos de licença

Siga estes passos para instalar as licenças dos switches de cluster BES-53248.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o EFOS, as licenças e o arquivo RCF.

Mostrar exemplo

Este exemplo verifica se o switch está conectado 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 o uso atual da licença no switch 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 arquivo de licença.

Repita este passo para carregar mais licenças e usar números de índice de chave diferentes.

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 de licença atuais e observe o status da licença antes de reiniciar o switch CS2:

```
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
```

Actor		Admin	Physical	Physical	Link	Link	LACP
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 confirme 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
```

Actor		Admin	Physical	Physical	Link	Link	LACP
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 reapply um RCF em uma chave de produção já em funcionamento.

Solucionar problemas de instalação

Caso surjam problemas durante a instalação da licença, execute os seguintes comandos de depuração antes de executar o programa. `copy` Comande novamente.

Comandos de depuração a serem usados: `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 o `debug transfer` e `debug license` Com as opções ativadas, o resultado do log é retornado.

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 interruptor corresponde: Model BES-53248 matched.
- Verifique se o índice de licença especificado não foi usado anteriormente. Quando um índice de licença já está em uso, o seguinte erro é retornado: License file /mnt/download//license.dat.1 already exists.
- Uma licença de porta não é uma licença de funcionalidade. Portanto, espera-se a seguinte afirmação: Feature not found in license file with index = 1.

Use o copy comando para fazer backup das licenças de porta no servidor:


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



Se precisar fazer o downgrade do software do switch da versão 3.4.4.6, as licenças serão removidas. Este é o comportamento esperado.

Você precisa instalar uma licença antiga apropriada antes de reverter para uma versão anterior do software.

Ativar portas recém-licenciadas

Para ativar as portas recém-licenciadas, você precisa editar a versão mais recente do RCF e remover o comentário dos detalhes da porta em questão.

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 e 0/54, dependendo do tipo e da quantidade de licenças disponíveis. Por exemplo, para ativar a licença SW-BES54248-40-100G-LIC, você deve remover o comentário da 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, remova o comentário de cada porta, mas remova apenas uma linha **speed** no arquivo 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, remova o comentário de toda a seção de 8 portas quando uma licença apropriada tiver sido ativada.

O que vem a seguir?

Após instalar as licenças, você pode ["Instale o arquivo de configuração de referência \(RCF\)."](#) ou ["atualizar RCF"](#).

Instale o arquivo de configuração (RCF)

Você pode instalar o RCF após configurar o switch de cluster BES-53248 e após aplicar as novas licenças.



Para o EFOS 3.12 e versões posteriores, siga os passos de instalação em ["Instale o arquivo de configuração \(RCF\) e o arquivo de licença"](#).

Requisitos de revisão

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 ["Comutadores de cluster Broadcom"](#) página.
- Uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas, necessária caso você esteja instalando apenas o EFOS e mantendo sua versão atual do RCF. Se 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 reinicializações futuras.
- É necessária uma conexão de console com o switch ao instalar o RCF a partir de suas configurações de fábrica. Este requisito é opcional caso você tenha utilizado o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#) para limpar a configuração, previamente.

Documentação sugerida

Consulte a tabela de compatibilidade de switches para as versões suportadas do ONTAP e do RCF. Consulte ["Download do software EFOS"](#). Observe que pode haver dependências de comandos entre a sintaxe de comandos no RCF e a encontrada nas versões do EFOS.

Instale o arquivo de configuração.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do 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::*>` O 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 a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Sobre esta tarefa

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

Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e RCFs, use o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#). Se for necessário apagar completamente as configurações do switch, será preciso realizar a configuração básica novamente. Você deve estar conectado ao switch usando o console serial, pois uma exclusão 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, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

O comando a seguir 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.
 - a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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					
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
```

Health	Health				Speed (Mbps)	
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 principal:

```
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	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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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. [[passo 6]]Desative a 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 conectadas aos nós do cluster.

```
show isdp neighbor
```

2. No switch de cluster cs2, desligue as portas conectadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conectadas 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 as LIFs do cluster foram migradas 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::*>				

4. Verifique se o cluster está íntegro:

```
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. Caso ainda não o tenha feito, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração do switch CS2 e execute uma configuração básica.



Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial para apagar as configurações do switch. Este requisito é opcional se você já utilizou o artigo da Base de Conhecimento. ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota?"](#) Para limpar a configuração previamente.



Limpar a configuração não exclui as licenças.

- a. Acesse o switch via SSH.

Prossiga somente quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para ter a configuração apagada.

- b. Entrar no modo privilegiado:

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

- c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior utilizada, alguns comandos podem gerar um erro se uma determinada configuração 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 um reinício do switch:

```
(cs2)# reload
```

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

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

7. Observe o seguinte:

- a. Se licenças de porta adicionais tiverem sido instaladas no switch, você deve modificar o RCF para configurar as portas licenciadas adicionais. Consulte ["Ativar portas recém-licenciadas"](#) para obter detalhes.
- b. Registre todas as personalizações feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, configurar as velocidades das portas ou programar o modo FEC.

EFOS versão 3.12.x e posterior

1. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: HTTP, HTTPS, FTP, TFTP, SFTP ou SCP.

Este exemplo mostra o uso do SFTP para copiar um arquivo RCF para a memória 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 com o nome de arquivo que você definiu:

```
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 interruptor:

```
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 EFOS

1. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: HTTP, HTTPS, FTP, TFTP, SFTP ou SCP.

Este exemplo mostra o uso do SFTP para copiar um arquivo RCF para a memória 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 com o nome de arquivo que você definiu:

```
script list
```

```
(cs2)# script list
```

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

```
1 configuration script(s) found.
```

2. Aplique o script ao interruptor:

```
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 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 após a aplicação do RCF:

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

Mostrar exemplo

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

LACP	Actor	Admin	Physical	Physical	Link	Link
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 interruptor se as alterações foram aplicadas:

```
show running-config
```

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

4. Salve a configuração em execução para que ela se torne a configuração de inicialização ao 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, ative as portas conectadas às portas de cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conectadas 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
```

Media	Flow	Link	Physical	Physical	
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 do cluster.
 - a. Verifique se as portas e0b 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					
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 o estado de funcionamento do switch 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			

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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
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, desligue as portas conectadas às portas de cluster dos nós.

O exemplo a seguir utiliza a saída de exemplo da interface:

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

2. Verifique se as LIFs do cluster foram migradas 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	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 íntegro:

```
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 switch cs1.

5. Ativar reversão automática nos LIFs do cluster:

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

6. Reinicie o interruptor cs1. Isso faz com que as LIFs do cluster voltem às suas portas originais. Você pode ignorar os eventos de "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
(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!
```

Etapas 3: Verifique a configuração

1. No switch cs1, verifique se as portas do switch conectadas às portas do cluster estão **ativas**:

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

Mostrar exemplo

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

Media	Flow	Link	Physical	Physical	
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 switches cs1 e cs2 está funcionando corretamente:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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	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 íntegro:

```
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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 administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Após instalar o RCF, você pode "[habilitar SSH](#)".

Habilite o SSH nos switches de cluster BES-53248.

Se você estiver usando o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de coleta de logs, será necessário gerar as chaves SSH e, em seguida, habilitar 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 desativado, desative-o da seguinte forma:

```
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 desativar o SSH antes de modificar as chaves; caso contrário, um aviso será exibido 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. Criptografe as chaves SSH (somente para o modo FIPS):



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

Mostrar exemplo

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

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  
<passphrase>
```

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  
<passphrase>
```

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 vem a seguir?

Depois de habilitar o SSH, você pode ["configurar monitoramento de integridade do switch"](#).

Redefinir o switch do 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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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 reiniciar o switch, selecione **Não**.

1. [[passo 4]] Aguarde o switch reiniciar e, em seguida, faça login no switch.

O usuário padrão é “admin” e nenhuma senha foi definida. Uma mensagem semelhante à seguinte é exibida:

```
(Routing) >
```

Atualize o switch

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

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

1

"Atualize sua versão do EFOS"

Faça o download e instale o software Ethernet Fabric OS (EFOS) no switch de cluster BES-53248.

2

"Atualize sua versão do RCF"

Atualize o RCF no switch de cluster BES-53248 e, em seguida, verifique se há uma licença adicional disponível nas portas após a aplicação do RCF.

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 do 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 recursos e protocolos de rede avançados para o desenvolvimento de sistemas de infraestrutura Ethernet e IP. Essa arquitetura de software é adequada para qualquer dispositivo de organização de rede que utilize aplicações que exijam inspeção ou separação minuciosa de pacotes.

Prepare-se para a atualização

Antes de começar

- Faça o download do software Broadcom EFOS aplicável aos switches do seu cluster no site "[Suporte para switches Ethernet Broadcom](#)".
- Consulte as seguintes notas referentes às versões do EFOS.

Observe o seguinte:

- Ao atualizar do EFOS 3.4.xx para o EFOS 3.7.xx ou posterior, o switch deve estar executando o EFOS 3.4.4.6 (ou uma versão 3.4.xx posterior). Se você estiver executando uma versão anterior a essa, atualize primeiro o switch para o EFOS 3.4.4.6 (ou uma versão 3.4.xx posterior) e, em seguida, atualize-o para o EFOS 3.7.xx ou posterior.
- A configuração para o EFOS 3.4.xx e para o 3.7.xx ou versões posteriores é diferente. Alterar a versão do EFOS de 3.4.xx para 3.7.xx ou posterior, ou vice-versa, exige que o switch seja redefinido para as configurações de fábrica e que os arquivos RCF da versão correspondente do EFOS sejam (re)aplicados. Este procedimento requer acesso através da porta de console serial.
- A partir da versão 3.7.xx ou posterior do EFOS, estão disponíveis uma versão não compatível com FIPS e uma versão compatível com FIPS. Etapas diferentes se aplicam ao migrar 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 as configurações de fábrica. Este procedimento requer acesso através da porta de console serial.

Procedimento	*Versão atual do EFOS *	Nova versão EFOS	Etapas de alto nível
Passos 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 EFOS . As informações de configuração e licença são mantidas.

3.4.4.6 (ou posterior 3.4.xx)	3.7.xx ou posterior não compatível com FIPS	Atualize o EFOS usando Método 1: Atualizar o EFOS . Restaure as configurações de fábrica do switch e aplique o arquivo RCF para EFOS 3.7.xx ou posterior.	3.7.xx ou posterior não compatível com FIPS
3.4.4.6 (ou posterior 3.4.xx)	Rebaixar EFOS usando Método 1: Atualizar o EFOS . Restaure as configurações de fábrica do switch e aplique o arquivo RCF para EFOS 3.4.xx.	3.7.xx ou posterior não compatível com FIPS	
Atualize a nova imagem EFOS usando Método 1: Atualizar o EFOS . As informações de configuração e licença são mantidas.	Compatível com FIPS versão 3.7.xx ou posterior	Compatível com FIPS versão 3.7.xx ou posterior	Atualize a nova imagem EFOS usando Método 1: Atualizar o EFOS . As informações de configuração e licença são mantidas.
Etapas para atualizar para/de uma versão do EFOS compatível com FIPS	Não compatível com FIPS	Em conformidade com o FIPS	Atualização da imagem EFOS usando Método 2: Atualizar o EFOS usando a instalação do ONIE OS . As informações de configuração e licença do switch serão perdidas.


```
System running in FIPS mode
```

```

% Invalid input detected at ^ marker.

```



```
(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. Exibir as imagens de inicialização para a configuração ativa e de backup:

```
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. Faça o download do arquivo de imagem para o switch.

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. Exibir as imagens de inicialização para a configuração ativa e de backup:

```
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      3.10.0.3          3.7.0.4          3.10.0.3
```

7. Inicialize o sistema a partir da configuração de backup:

```
boot system backup
```

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

8. Exibir as imagens de inicialização para a configuração ativa e de backup:

```
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. Faça login 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 interruptor cs1.
13. Ative a reversão automática nos LIFs do cluster.

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

14. Verifique se as LIFs do cluster retornaram à sua porta original:

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

Para obter mais detalhes, consulte ["Reverter um LIF para sua porta de origem"](#).

Método 2: Atualizar o EFOS usando a instalação do ONIE OS

Você pode executar os seguintes passos se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS. Esses passos podem ser usados para atualizar a imagem EFOS 3.7.xx, compatível ou não com FIPS, a partir do ONIE, caso o switch não inicialize.



Essa funcionalidade está disponível apenas para EFOS 3.7.xx 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 precisa configurar o switch, instalar as licenças e um RCF compatível para que o switch volte a operar normalmente.

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 a inicialização, selecione ONIE quando a mensagem aparecer:

```

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

```

Após selecionar **ONIE**, o interruptor carrega e apresenta várias opções. Selecione **Instalar SO**.

```

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

```

O switch inicia no modo de instalação ONIE.

3. Interrompa a descoberta ONIE e configure a interface Ethernet.

Quando a seguinte mensagem aparecer, pressione **Enter** para abrir o console ONIE:

```

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

```



A detecção do 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 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 do 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 switch:

```
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 é instalado e, em seguida, reinicia o switch. Deixe o switch reiniciar normalmente na 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 reinicia sem nenhuma configuração aplicada e retorna às configurações de fábrica. Siga os passos abaixo para reconfigurar o switch:

- a. ["Instalar licenças"](#)
- b. ["Instale o RCF"](#)
- c. ["Habilitar SSH"](#)
- d. ["Ativar coleta de logs"](#)

e. ["Configure o SNMPv3 para monitoramento."](#)

9. Repita os passos 2 a 8 no interruptor cs1.

10. Ative a reversão automática nos LIFs do cluster.

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

11. Verifique se as LIFs do cluster retornaram à sua porta original:

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

Para obter mais detalhes, consulte ["Reverter um LIF para sua porta de origem"](#).

Atualizar a versão RCF

Você pode atualizar o RCF após atualizar o BES-53248 cluster switch EFOS e após aplicar quaisquer novas licenças.

Antes de começar

Certifique-se de ter o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O arquivo RCF atual está disponível em ["Comutadores de cluster Broadcom"](#) página.
- Uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas, necessária caso você esteja instalando apenas o EFOS e mantendo sua versão atual do RCF. Se 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 reinicializações futuras.
- É necessária uma conexão de console com o switch ao instalar o RCF a partir de suas configurações padrão de fábrica. Este requisito é opcional se você já utilizou o artigo da Base de Conhecimento. ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#) Para limpar a configuração previamente.

Documentação sugerida

- Consulte a tabela de compatibilidade de switches para as versões suportadas do ONTAP e do RCF. Consulte ["Download do software EFOS"](#). Observe que pode haver dependências de comandos entre a sintaxe de comandos no RCF e a encontrada nas versões do EFOS.
- Consulte os guias de software e upgrade disponíveis no ["Broadcom"](#) site para obter a documentação completa sobre os procedimentos de upgrade e downgrade do switch BES-53248.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do 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::*>` O 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 a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Sobre esta tarefa

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

Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software de switch e RCFs, consulte o artigo da Base de Conhecimento. ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota"](#). Se precisar apagar completamente as configurações do switch, será necessário realizar a configuração básica novamente. Você precisa estar conectado ao switch usando o console serial, pois a exclusão completa da configuração redefine a configuração da rede de gerenciamento.

Etapa 1: Prepare-se para a atualização

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

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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

O comando a seguir 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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					
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
```

```
Health      Health      Speed (Mbps)
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 principal:

```
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	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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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. [[passo 6]]Desative a 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 conectadas aos nós do cluster.

```
show isdp neighbor
```

2. No switch cs2, desligue as portas conectadas às portas do cluster dos nós. Por exemplo, se as portas 0/1 a 0/16 estiverem conectadas 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 as LIFs do cluster foram migradas 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::*>
```

4. Verifique se o cluster está íntegro:

```
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. Caso ainda não o tenha feito, salve a configuração atual do switch copiando a saída do seguinte comando para um arquivo de log:

```
show running-config
```

6. Limpe a configuração do switch CS2 e execute uma configuração básica.



Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial para apagar as configurações do switch. Este requisito é opcional se você já utilizou o artigo da Base de Conhecimento. ["Como limpar a configuração de um switch de interconexão Broadcom mantendo a conectividade remota?"](#) Para limpar a configuração previamente.



Limpar a configuração não exclui as licenças.

- a. Acesse o switch via SSH.

Prossiga somente quando todas as LIFs do cluster tiverem sido removidas das portas do switch e o switch estiver preparado para ter a configuração apagada.

- b. Entrar no modo privilegiado:

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

- c. Copie e cole os seguintes comandos para remover a configuração RCF anterior (dependendo da versão RCF anterior utilizada, alguns comandos podem gerar um erro se uma determinada configuração 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 um reinício do switch:

```
reload
```

```
(cs2)# reload
```

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

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

7. Observe o seguinte:

- a. Se licenças de porta adicionais tiverem sido instaladas no switch, você deve modificar o RCF para configurar as portas licenciadas adicionais. Consulte ["Ativar portas recém-licenciadas"](#) para obter detalhes. No entanto, ao atualizar para o RCF 1.12 ou posterior, as modificações não são mais necessárias porque todas as interfaces agora estão pré-configuradas.
- b. Registre todas as personalizações feitas no RCF anterior e aplique-as ao novo RCF. Por exemplo, configurar as velocidades das portas ou programar o modo FEC.

EFOS versão 3.12.x e posterior

1. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: HTTP, HTTPS, FTP, TFTP, SFTP ou SCP.

Este exemplo mostra o uso do SFTP para copiar um arquivo RCF para a memória 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 com o nome de arquivo que você definiu:

```
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 interruptor:

```
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 EFOS

1. Copie o RCF para o bootflash do switch cs2 usando um dos seguintes protocolos de transferência: HTTP, HTTPS, FTP, TFTP, SFTP ou SCP.

Este exemplo mostra o uso do SFTP para copiar um arquivo RCF para a memória 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 com o nome de arquivo que você definiu:

```
script list
```

```
(cs2)# script list
```

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

```
1 configuration script(s) found.
```

2. Aplique o script ao interruptor:

```
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. **[[passo 11]]**Examine a saída do banner do `show clibanner` comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas 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 após a aplicação do RCF:

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

Mostrar exemplo

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

LACP	Actor	Admin	Physical	Physical	Link	Link
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 interruptor se as alterações foram aplicadas.

```
show running-config
```

4. Salve a configuração em execução para que ela se torne a configuração de inicialização ao 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, ative as portas conectadas 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
```

Media	Flow	Link	Physical	Physical	
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 do cluster.

a. Verifique se as portas e0b 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					
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 o estado de funcionamento do switch no cluster:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

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 9.8 e posterior

A partir do ONTAP 9.8, utilize 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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
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 interruptor cs1.
2. Ativar reversão automática nos LIFs do cluster:

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

3. . Verifique se as LIFs do cluster retornaram à sua porta original:

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

Para obter mais detalhes, consulte ["Reverter um LIF para sua porta de origem"](#).

Etapa 3: Verifique a configuração

1. No switch cs1, verifique se as portas do switch conectadas às portas do cluster estão **ativas**:

```
show interfaces status all
```

Mostrar exemplo

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

Media	Flow	Link	Physical	Physical	
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 switches cs1 e cs2 está funcionando corretamente:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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	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 íntegro:

```
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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 administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do 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 de cluster BES-53248.

Você pode usar os seguintes comandos para verificar a integridade da rede do cluster ONTAP após uma atualização do software EFOS ou do 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`deve ter o valor `up e Health Status deve 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` é `true` e `Status Admin/Oper` é `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 é true usando o comando:

```
cluster show
```

Mostrar exemplo

```
cluster1::> cluster show
```

Node	Health	Eligibility	Epsilon

node1	true	true	false
node2	true	true	false

O que vem a seguir?

Após confirmar a atualização do seu software EFOS ou RCF, você pode ["configurar monitoramento de integridade do switch"](#).

Migre os switches

Migrar switches de cluster CN1610 para switches de cluster BES-53248

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

migração.

Os seguintes switches de cluster são suportados:

- CN1610
- BES-53248

Requisitos de revisão

Verifique se sua configuração atende aos seguintes requisitos:

- Algumas portas dos switches BES-53248 estão configuradas para operar em 10GbE.
- A conectividade 10GbE dos nós aos switches de cluster BES-53248 foi planejada, migrada e documentada.
- O cluster está funcionando perfeitamente (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 arquivos de configuração de referência (RCFs) foram aplicados aos switches.
 - Qualquer personalização do site, como DNS, NTP, SMTP, SNMP e SSH, é configurada nos novos switches.

Conexões de nós

Os switches de cluster suportam as seguintes conexões de nó:

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



É possível ativar portas adicionais adquirindo licenças de porta.

Portas ISL

Os switches do cluster utilizam as seguintes portas de enlace entre switches (ISL):

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

O ["Hardware Universe"](#) contém informações sobre compatibilidade com ONTAP, firmware EFOS suportado e cabeamento para switches de cluster BES-53248. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para mais informações sobre os requisitos de instalação do switch.

Cabeamento ISL

A cablagem ISL adequada é a seguinte:

- **Início:** Para CN1610 para CN1610 (SFP+ para SFP+), quatro cabos de fibra óptica ou cobre SFP+ de conexão direta.
- **Final:** Para BES-53248 para BES-53248 (QSFP28 para QSFP28), dois transceptores ópticos QSFP28/cabos de fibra ou cobre de conexão direta.

Migre os switches

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

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os exemplos utilizam dois nós, cada um com duas portas de interconexão de cluster de 10 GbE: e0a e e0b .
- Os resultados dos comandos podem variar dependendo das diferentes versões do software ONTAP .
- Os interruptores CN1610 a serem substituídos são: CL1 e CL2 .
- Os switches BES-53248 substituem os switches CN1610. cs1 e cs2 .
- Os nós são node1 e node2 .
- O interruptor CL2 é substituído primeiro por cs2, seguido por CL1, que é substituído por cs1.
- Os switches BES-53248 vêm pré-carregados com as versões suportadas do Reference Configuration File (RCF) e do Ethernet Fabric OS (EFOS), com cabos ISL conectados nas portas 55 e 56.
- Os nomes LIF do cluster são node1_clus1 e node1_clus2 para o nó 1 e node2_clus1 e node2_clus2 para o nó 2.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O cluster inicia com dois nós conectados a dois switches de cluster CN1610.
- O switch CN1610 CL2 foi substituído pelo switch BES-53248 cs2:
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Desconecte os cabos de todas as portas do cluster em todos os nós conectados ao CL2 e, em seguida, use cabos compatíveis para reconectar as portas ao novo switch de cluster cs2.
- O switch CN1610 CL1 foi substituído pelo switch BES-53248 cs1:
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Desconecte os cabos de todas as portas do cluster em todos os nós conectados ao CL1 e, em seguida, use cabos compatíveis para reconectar as portas ao novo switch de cluster cs1.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Etapa 1: Prepare-se para a migração

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

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


onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

O comando a seguir 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

Etapas 2: Configurar portas e cabos

1. Nos novos switches, confirme se o cabo ISL está conectado e funcionando corretamente entre os switches cs1 e cs2:

```
show port-channel
```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão **ativas** 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 estão **ativas** 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. Exibir as portas do cluster em cada nó conectado 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
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 um healthy status:

```
network port show -ipSPACE Cluster
```

Mostrar exemplo

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 de origem:

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

Mostrar exemplo

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

Current Is	Logical	Status	Network	Current
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 9.8 e posterior

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

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-is-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 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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. [[passo 5]]Desative a reversão automática nos LIFs do cluster.

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

2. No switch de cluster CL2, desligue as portas conectadas às portas de cluster dos nós para realizar o failover das LIFs do 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 do cluster foram transferidas 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 íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
```

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

- 5. Transfira todos os cabos de conexão dos nós do cluster do switch CL2 antigo para o novo switch CS2.
- 6. Confirme a integridade das conexões de rede migradas 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 do cluster que foram movidas devem ser up .

7. Verifique as informações dos vizinhos 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
53248			BES-
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	cs2	0/1
53248			BES-

8. Confirme se as conexões das portas do switch estão íntegras do ponto de vista do switch CS2:

```
cs2# show interface all
cs2# show isdp neighbors
```

9. No switch de cluster CL1, desligue as portas conectadas às portas de cluster dos nós para realizar o failover das LIFs do 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) #
```

Todas as LIFs do cluster fazem failover para o switch cs2.

10. Verifique se os LIFs do cluster falharam nas 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 íntegro:

```
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 o estado 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 do cluster que foram movidas devem ser up .

14. Verifique as informações dos vizinhos 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
53248			BES-
	e0b	cs2	0/1
53248			BES-
node2	/cdp		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-

15. Confirme se as conexões das portas do switch estão íntegras 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 estão **ativas** 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 estão **ativas** 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, caso eles não sejam removidos

automaticamente:

ONTAP 9.8 e posterior

A partir do ONTAP 9.8, utilize o comando: `system switch ethernet delete -device device-name`

```
cluster::*> system switch ethernet delete -device CL1
cluster::*> system switch ethernet delete -device CL2
```

ONTAP 9.7 e versões anteriores

Para ONTAP 9.7 e versões anteriores, utilize 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. No switch cs2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

```
cs2> enable
cs2# configure
cs2(config)# interface 0/1-0/16
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

3. Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verifique se o cluster está íntegro:

```
cluster show
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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		

Todas as versões do ONTAP

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

```
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. [[passo 6]]Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migre para um ambiente de cluster NetApp comutado.

Se você já possui um ambiente de cluster de dois nós sem switches, pode migrar para um ambiente de cluster de dois nós com switches usando os switches de cluster BES-53248 compatíveis com a Broadcom, o que permite escalar o cluster para além de dois nós.

O processo de migração funciona para todas as portas de nós do cluster que utilizam portas ópticas ou Twinax, mas não é suportado neste switch se os nós estiverem utilizando portas RJ45 10GBASE-T integradas

para as portas de rede do cluster.

Requisitos de revisão

Analise os seguintes requisitos para o ambiente de cluster.

- Tenha em mente que a maioria dos sistemas requer duas portas de rede dedicadas para o cluster em cada controlador.
- Certifique-se de que o comutador de cluster BES-53248 esteja configurado conforme descrito em ["Requisitos de substituição"](#) 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 configurada corretamente e funcionando.
 - Os nós estão executando o ONTAP 9.5P8 ou versões posteriores. O suporte para portas de cluster 40/100 GbE começa com a versão 3.4.4.6 e posteriores do firmware EFOS.
 - Todas as portas do cluster estão no estado **ativo**.
 - Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e em suas portas de origem.
- Para a configuração do switch de cluster BES-53248 com suporte da Broadcom, certifique-se de que:
 - O comutador de cluster BES-53248 está totalmente funcional em ambos os comutadores.
 - Ambos os switches possuem conectividade de rede de gerenciamento.
 - É possível acessar os switches do cluster através do console.
 - As conexões entre nós e entre switches do BES-53248 utilizam cabos Twinax ou de fibra óptica.

O ["Hardware Universe"](#) contém informações sobre compatibilidade com ONTAP, firmware EFOS suportado e cabeamento para switches BES-53248. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para mais informações sobre os requisitos de instalação do switch.

- Os cabos Inter-Switch Link (ISL) são conectados 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 possuem licenças de porta opcionais instaladas, caso sejam adquiridas.
 - Os arquivos de configuração de referência (RCFs) são aplicados aos switches.
- Qualquer personalização do site (SMTP, SNMP e SSH) é configurada nos novos switches.

restrições de velocidade do grupo portuário

- As 48 portas 10/25GbE (SFP28/SFP+) são combinadas em 12 grupos de 4 portas, da seguinte forma: Portas 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 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 neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- 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, respectivamente.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são `e0a` e `e0b`.

O "[Hardware Universe](#)" contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

Etapa 1: Prepare-se para a migração

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

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

O comando a seguir 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado(`*>`) aparece.

Etapa 2: Configurar portas e cabos

1. Desative todas as portas voltadas para o nó que estiverem ativadas (exceto as portas ISL) nos dois novos switches do cluster, `cs1` e `cs2`.



Você não deve desativar as portas ISL.

O exemplo a seguir mostra que as portas voltadas para o nó, de 1 a 16, 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 ativas 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 estão ativas 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
```

3. Exibir a lista de dispositivos vizinhos:

```
show isdp neighbors
```

Este comando fornece informações sobre os dispositivos que estão conectados 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 -ip space Cluster
```

Mostrar exemplo

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

Node: node1

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

Node: node2

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

5. Verifique se todas as LIFs do 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. Desconecte o cabo da porta do cluster e0a no nó 1 e, em seguida, conecte e0a à porta 1 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches BES-53248.

O "[Hardware Universe](#)" documento contém mais informações sobre cabeamento.

8. Desconecte o cabo da porta do cluster e0a no nó 2 e, em seguida, conecte e0a à porta 2 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches BES-53248.

9. Habilite todas as portas voltadas para os nós no switch de cluster cs1.

O exemplo a seguir mostra que as portas de 1 a 16 estão habilitadas 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 do 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					

12. Exibir informações sobre o estado 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

- Desconecte o cabo da porta do cluster e0b no nó 1 e, em seguida, conecte e0b à porta 1 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches BES-53248.
- Desconecte o cabo da porta do cluster e0b no nó 2 e, em seguida, conecte e0b à porta 2 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches BES-53248.
- Habilite todas as portas voltadas para os nós no switch de cluster cs2.

O exemplo a seguir mostra que as portas de 1 a 16 estão habilitadas 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. No switch cs2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

```
cs2> enable  
cs2# configure  
cs2(config)# interface 0/1-0/16  
cs2(config-if-range)# shutdown  
  
(Wait for 5-10 seconds before re-enabling the ports)  
  
cs2(config-if-range)# no shutdown  
  
(After executing the no shutdown command, the nodes detect the change  
and begin to auto-revert the cluster LIFs to their home ports)  
  
cs2(config-if-range)# exit  
cs2(config)# exit  
cs2#
```

3. Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verifique se todas as interfaces exibem `true` para `Is Home`:

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



Isso pode levar alguns 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					

5. Verifique se ambos os nós possuem uma conexão com cada switch:

```
show isdp neighbors
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
(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

6. Exibir 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		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-

7. Verifique se as configurações estão desativadas:

```
network options switchless-cluster show
```



A conclusão do comando pode levar alguns minutos. Aguarde o anúncio de que o tempo de vida de 3 minutos está prestes a expirar.

O false O resultado no exemplo a seguir mostra que as configurações estão desativadas:

```
cluster1::*> network options switchless-cluster show
```

Enable Switchless Cluster: **false**

8. Verifique o status dos nós membros do cluster:

```
cluster show
```


Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show
```

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

9. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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		

Todas as versões do ONTAP

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

```
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. **[[passo 10]]**Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

Mostrar exemplo

```

cluster1::*> system node autosupport invoke -node * -type all
-messsage MAINT=END

```

Para obter mais informações, consulte: ["Artigo da Base de Conhecimento da NetApp : Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#)

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Substitua os interruptores

Requisitos de substituição

Antes de substituir o switch, certifique-se de que as seguintes condições sejam atendidas no ambiente atual e no switch de substituição.

Infraestrutura de cluster e rede existente

Certifique-se de que:

- O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
- Todas as portas do cluster estão **ativas**.
- Todas as interfaces lógicas do cluster (LIFs) estão administrativa e operacionalmente **ativas** e em suas portas de origem.
- O ONTAP `cluster ping-cluster -node node1` O comando deve indicar as configurações, `basic connectivity` e `larger than PMTU communication`, são bem-sucedidos em todos os caminhos.

Interruptor de substituição do cluster BES-53248

Certifique-se de que:

- A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
- O acesso ao console para o interruptor de substituição já está instalado.
- As conexões de nó são feitas nas portas 0/1 a 0/16 com licenciamento padrão.
- Todas as portas de Interconexão de Switches (ISL) estão desativadas nas portas 0/55 e 0/56.
- O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional EFOS são carregados no switch.
- A personalização inicial do interruptor está concluída, conforme detalhado em ["Configurar o switch de cluster BES-53248"](#).

Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, são copiadas para o novo switch.

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Informações relacionadas

- ["Site de suporte da NetApp"](#)
- ["Hardware Universe da NetApp"](#)

Substitua um switch de cluster BES-53248 compatível com Broadcom

Siga estes passos para substituir um switch de cluster BES-53248 com defeito e compatível com a Broadcom em uma rede de cluster. Este é um procedimento não disruptivo (NDU).

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster em cada nó são nomeadas. `e0a` e `e0b` .
- Os nomes LIF do cluster são `node1_clus1` e `node1_clus2` para o nó 1 e `node2_clus1` e `node2_clus2` para o nó 2.
- O aviso para alterações em todos os nós do cluster é `cluster1::>`

Sobre a topologia

Este procedimento baseia-se na seguinte topologia de rede em 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/ Protocol	Local Port	Discovered 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 Port ID	Intf	Holdtime	Capability	Platform
node1 e0a	0/1	175	H	FAS2750
node2 e0a	0/2	152	H	FAS2750
cs2 0/55	0/55	179	R	BES-53248
cs2 0/56	0/56	179	R	BES-53248

```
(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 Port ID	Intf	Holdtime	Capability	Platform
node1 e0b	0/1	129	H	FAS2750
node2 e0b	0/2	165	H	FAS2750
cs1 0/55	0/55	179	R	BES-53248
cs1 0/56	0/56	179	R	BES-53248

Passos

1. Analise o ["Requisitos de substituição"](#) .
2. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :


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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

3. Instale o arquivo de configuração de referência (RCF) e a imagem apropriados no switch, newcs2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e EFOS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e EFOS, continue para a etapa 2.

- a. Você pode baixar o software Broadcom EFOS aplicável aos seus switches de cluster a partir do site ["Suporte para switches Ethernet Broadcom"](#) site. Siga os passos na página de Download para baixar o arquivo EFOS correspondente à versão do software ONTAP que você está instalando.
 - b. O RCF apropriado está disponível em ["Comutadores de cluster Broadcom"](#) página. Siga os passos na página de Download para baixar o RCF correto para a versão do software ONTAP que você está instalando.
4. No novo switch, faça login como `admin` e desative todas as portas que serão conectadas às interfaces do cluster de nós (portas 1 a 16).



Se você adquiriu licenças adicionais para portas adicionais, desative também essas portas.

Se o switch que você está substituindo não estiver funcionando e estiver desligado, as LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em cada nó.



Não é necessário senha para entrar. `enable` 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 todos os LIFs do cluster têm `auto-revert` habilitado:

```
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. Desative as portas ISL 0/55 e 0/56 no switch 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, em seguida, conecte-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, em seguida, verifique o status da operação do canal da porta.

O estado do link para o canal de porta 1/1 deve ser **ativo** e todas as portas membro devem estar com o status Verdadeiro na seção Porta Ativa.

Mostrar exemplo

Este exemplo habilita as portas ISL 0/55 e 0/56 e exibe o estado do link para o canal de porta 1/1 no switch 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 conectadas às interfaces do cluster de nós (portas 1 a 16).



Se você adquiriu licenças adicionais para portas adicionais, desative também essas portas.

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 está **ativa**:

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

Mostrar exemplo

O resultado deverá ser semelhante ao seguinte:

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

Node: node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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 usado na etapa anterior, aguarde a reversão automática do LIF do cluster node1_clus2 no nó 1.

Mostrar exemplo

Neste exemplo, o LIF node1_clus2 no nó 1 é revertido com sucesso se Is Home é true e a porta é e0b.

O comando a seguir exibe informações sobre as LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se Is Home é true para ambas as interfaces do cluster e elas mostram as atribuições de porta corretas, neste exemplo. e0a e e0b no nó 1.

```
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 a saúde do nó para node1 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 do 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 íntegra:

```
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 desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Substitua os switches de cluster Broadcom BES-53248 por conexões sem switch.

É possível migrar de um cluster com uma rede de cluster comutada para uma em que

dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

Requisitos de revisão

Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

Antes de começar

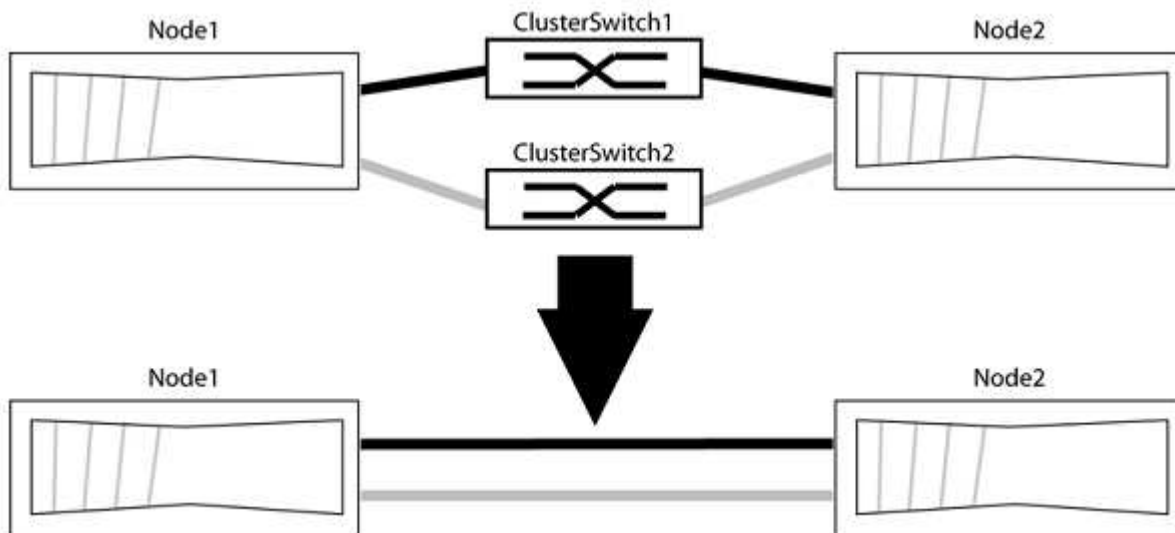
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migre 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 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 elas variam de acordo com o sistema.

Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

onde `h` é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período 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 cabos

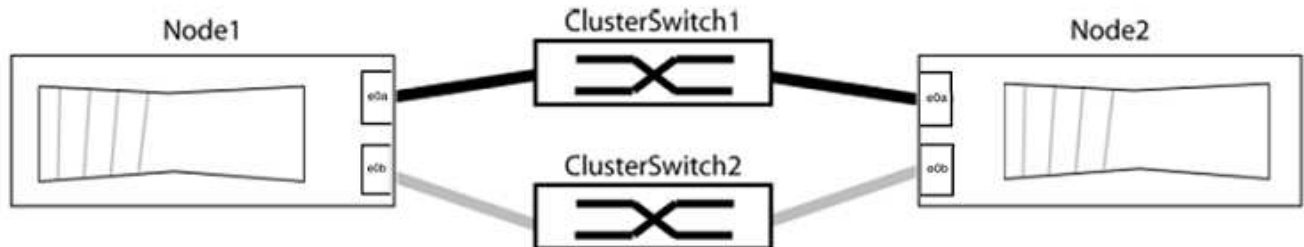
1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de

cluster 2. Esses grupos serão necessários mais tarde no procedimento.

2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Estado de Saúde".

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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está `true` para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

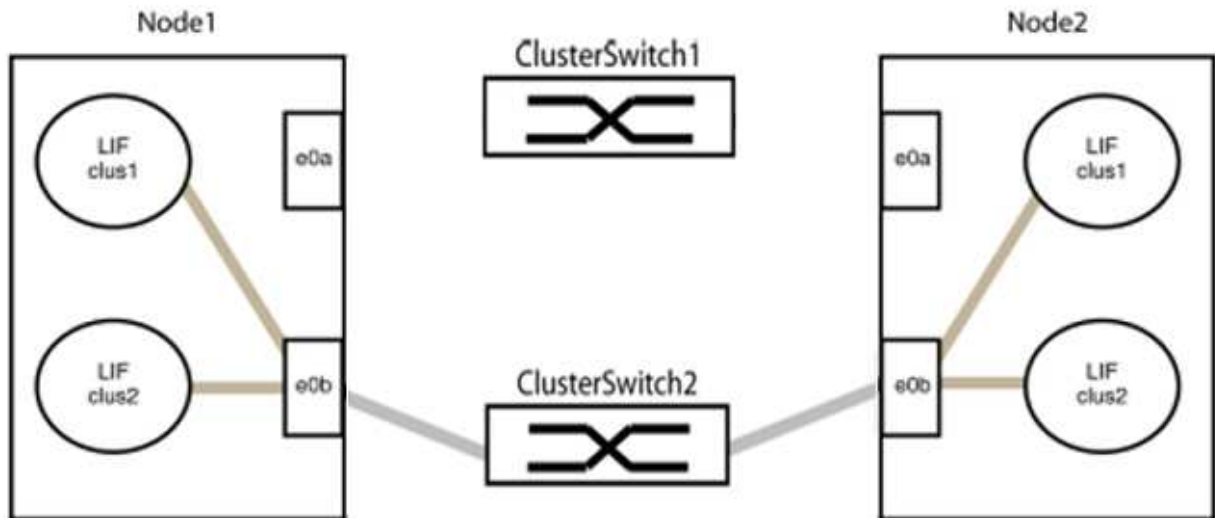
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

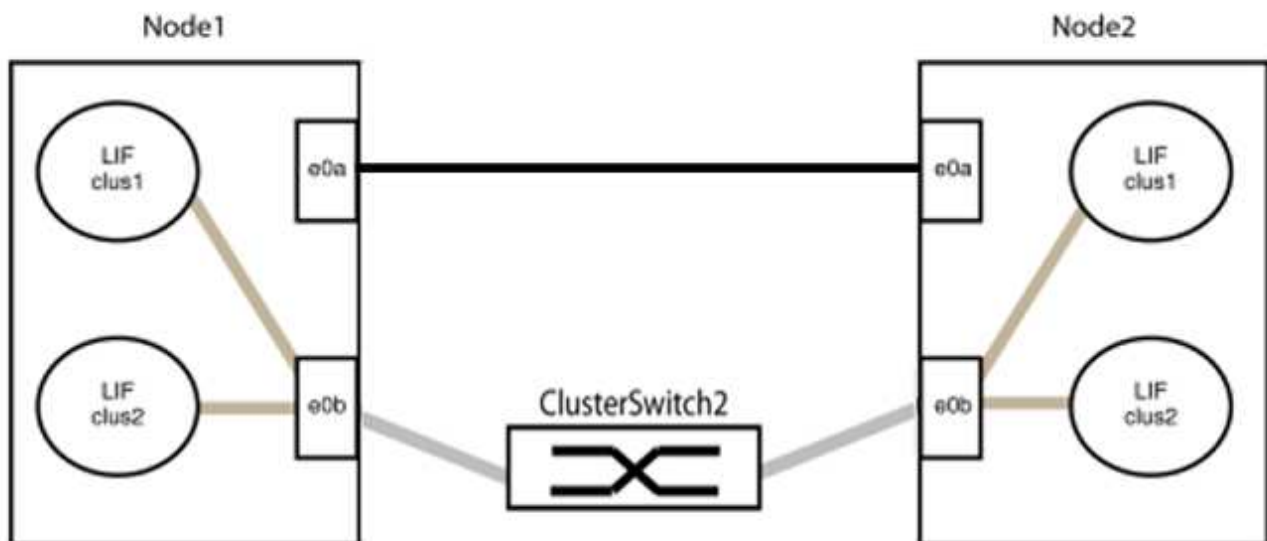
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

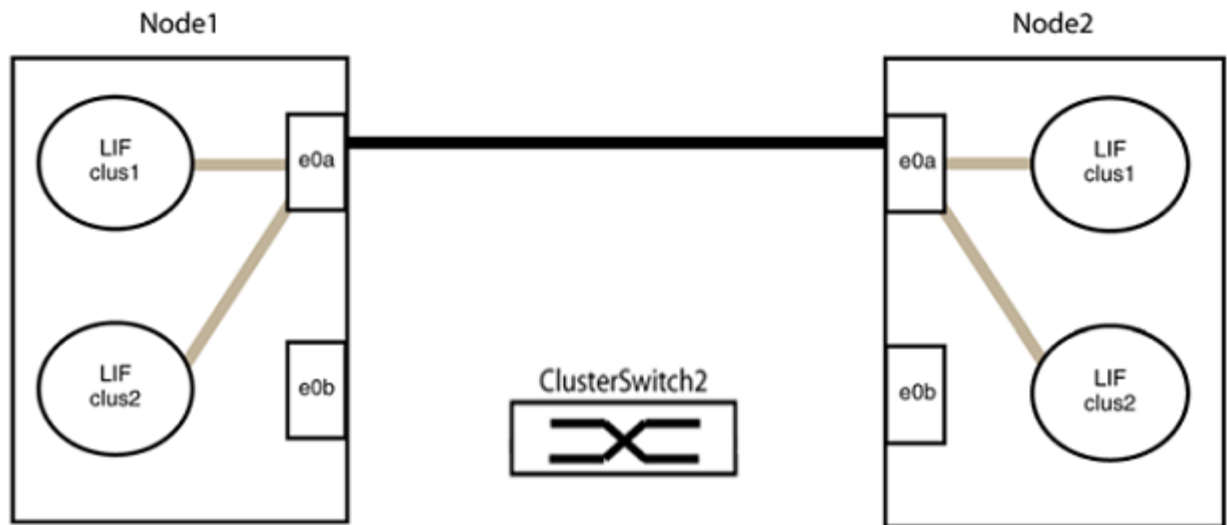
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna “Is Home” estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 6]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Cisco Nexus 9336C-FX2 ou 9336C-FX2-T

Começar

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.

ONTAP 9.9.1 e posterior

A partir do ONTAP 9.9.1, você pode usar switches Cisco Nexus 9336C-FX2 para combinar funcionalidades de armazenamento e cluster em uma configuração de switch compartilhada.

Se você deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.



O monitor de integridade do switch Ethernet não é compatível com ONTAP 9.13.1P8 e versões anteriores, 9.14.1P3 e versões 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 deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

Requisitos de configuração

Certifique-se de que:

- Você possui a quantidade e o tipo adequados de cabos e conectores para seus switches. Consulte o ["Hardware Universe"](#).
- Dependendo do tipo de switch que você está configurando inicialmente, você precisa se conectar à porta do console do switch com o cabo de console incluído.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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 o ["Hardware Universe"](#) para obter as informações mais recentes.

Para obter mais informações sobre a configuração inicial do seu switch, consulte o seguinte ["Guia de Instalação e Atualização do Cisco Nexus 9336C-FX2"](#).

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["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 dos switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T,

certifique-se de consultar a lista de componentes e números de peça.

Detalhes do número da peça

A tabela a seguir lista o número da peça e a descrição dos switches, ventiladores e fontes de alimentação 9336C-FX2 e 9336C-FX2-T:

Número da peça	Descrição
X190200-CS-PE	Chave seletora de cluster, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Cluster Switch, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Chave seletora de cluster, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G
X190212-CS-PI	Chave seletora de cluster, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	SW, Licença Cisco 9336CFX2 POD de 24 portas
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	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de exaustão lateral
X-NXA-PAC-1100W-PI2	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de entrada pelo lado da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65 CFM, fluxo de ar de exaustão do lado esquerdo
X-NXA-FAN-65CFM-PI	N9K-9336C 65 CFM, fluxo de ar de admissão pelo lado esquerdo

Licenças Cisco Smart somente para portas 9336C-FX2-T

Para ativar mais de 12 portas no seu switch de cluster Cisco Nexus 9336C-FX-T, você precisa adquirir uma licença Cisco Smart. As licenças Cisco Smart são gerenciadas por meio de contas Cisco Smart.

1. Crie uma nova conta Smart, se necessário. Consulte ["Crie uma nova conta Smart"](#) para obter detalhes.
2. Solicite acesso a uma conta Smart existente. Consulte ["Solicitar acesso a uma conta Smart existente"](#) para obter detalhes.



Após adquirir sua licença Smart, instale o RCF apropriado para habilitar e configurar todas as 36 portas disponíveis para uso.

O que vem a seguir

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para a instalação 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 e 9336C-FX2-T, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 9000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 9000</i>	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 9000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 9000 Series NX-OS</i>	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 9000</i>	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 9000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 9000</i>	Descreve as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
<i>Notas de versão do NX-OS para a série Cisco Nexus 9000</i> (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.

Título do documento	Descrição
Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 9000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornece informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornece informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco 9336-FX2 em um NetApp cabinet, consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"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 do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale os switches 9336C-FX2 e 9336C-FX2-T.

3

"Instale o switch 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

"Revisar a cablagem e a configuração."

Revise o suporte para portas Ethernet NVIDIA , requisitos de FEC de 25 GbE e informações sobre recursos TCAM.

Preencha a planilha de cabeamento do Cisco Nexus 9336C-FX2 ou 9336C-FX2-T.

Se você deseja documentar as plataformas suportadas, baixe o PDF desta página e preencha a planilha de cabeamento.

A planilha de cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

- [Folha de exercícios de cabeamento de amostra 9336C-FX2](#)
- [Folha de trabalho de cabeamento em branco 9336C-FX2](#)
- [Folha de exemplo de cabeamento 9336C-FX2-T \(12 portas\)](#)

- [Folha de trabalho de cabeamento em branco 9336C-FX2-T \(12 portas\)](#)

Folha de exercícios de cabeamento de amostra 9336C-FX2

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 1 de 4x10GbE	1	Nó 1 de 4x10GbE
2	Nó 2 com 4x10GbE	2	Nó 2 com 4x10GbE
3	Nó 3 com 4x10GbE	3	Nó 3 com 4x10GbE
4	Nó 4x25GbE	4	Nó 4x25GbE
5	Nó 5 de 4x25GbE	5	Nó 5 de 4x25GbE
6	Nó 6 de 4x25GbE	6	Nó 6 de 4x25GbE
7	Nó 7 de 40/100GbE	7	Nó 7 de 40/100GbE
8	Nó 8 de 40/100GbE	8	Nó 8 de 40/100GbE
9	Nó 9 de 40/100GbE	9	Nó 9 de 40/100GbE
10	Nó 10 de 40/100GbE	10	Nó 10 de 40/100GbE
11	Nó 11 de 40/100GbE	11	Nó 11 de 40/100GbE
12	Nó 12 de 40/100GbE	12	Nó 12 de 40/100GbE
13	Nó 13 de 40/100GbE	13	Nó 13 de 40/100GbE
14	Nó 14 de 40/100GbE	14	Nó 14 de 40/100GbE
15	Nó 15 de 40/100GbE	15	Nó 15 de 40/100GbE
16	Nó 16 de 40/100GbE	16	Nó 16 de 40/100GbE
17	Nó 17 de 40/100GbE	17	Nó 17 de 40/100GbE
18	Nó 18 de 40/100GbE	18	Nó 18 de 40/100GbE
19	Nó 19 de 40/100GbE	19	Nó 19 de 40/100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
20	Nó 20 de 40/100GbE	20	Nó 20 de 40/100GbE
21	Nó 21 de 40/100GbE	21	Nó 21 de 40/100GbE
22	Nó 22 de 40/100GbE	22	Nó 22 de 40/100GbE
23	Nó 23 de 40/100GbE	23	Nó 23 de 40/100GbE
24	Nó 24 de 40/100GbE	24	Nó 24 de 40/100GbE
25 a 34	Reservado	25 a 34	Reservado
35	ISL de 100GbE para a porta 35 do switch B	35	ISL de 100GbE para switch A porta 35
36	ISL de 100GbE para a porta 36 do switch B	36	ISL de 100GbE para switch A porta 36

Folha de trabalho de cabeamento em branco 9336C-FX2

Você pode usar a planilha de cabeamento em branco para documentar as plataformas que são suportadas como nós em um cluster. A seção *Conexões de cluster suportadas* do "[Hardware Universe](#)" Define as portas do cluster utilizadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	

Chave seletora de cluster A		Chave seletora de cluster B	
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 34	Reservado	25 a 34	Reservado
35	ISL de 100GbE para a porta 35 do switch B	35	ISL de 100GbE para switch A porta 35
36	ISL de 100GbE para a porta 36 do switch B	36	ISL de 100GbE para switch A porta 36

Folha de exemplo de cabeamento 9336C-FX2-T (12 portas)

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas

Chave seletora de cluster A		Chave seletora de cluster B	
1	Nó 1 de 4x10GbE	1	Nó 1 de 4x10GbE
2	Nó 2 com 4x10GbE	2	Nó 2 com 4x10GbE
3	Nó 3 com 4x10GbE	3	Nó 3 com 4x10GbE
4	Nó 4x25GbE	4	Nó 4x25GbE
5	Nó 5 de 4x25GbE	5	Nó 5 de 4x25GbE
6	Nó 6 de 4x25GbE	6	Nó 6 de 4x25GbE
7	Nó 7 de 40/100GbE	7	Nó 7 de 40/100GbE
8	Nó 8 de 40/100GbE	8	Nó 8 de 40/100GbE
9	Nó 9 de 40/100GbE	9	Nó 9 de 40/100GbE
10	Nó 10 de 40/100GbE	10	Nó 10 de 40/100GbE
11 a 34	Requer licença	11 a 34	Requer licença
35	ISL de 100GbE para a porta 35 do switch B	35	ISL de 100GbE para switch A porta 35
36	ISL de 100GbE para a porta 36 do switch B	36	ISL de 100GbE para switch A porta 36

Folha de trabalho de cabeamento em branco 9336C-FX2-T (12 portas)

Você pode usar a planilha de cabeamento em branco para documentar as plataformas que são suportadas como nós em um cluster. A seção *Conexões de cluster suportadas* do "[Hardware Universe](#)" Define as portas do cluster utilizadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
1		1	
2		2	
3		3	
4		4	

Chave seletora de cluster A		Chave seletora de cluster B	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 a 34	Requer licença	11 a 34	Requer licença
35	ISL de 100GbE para a porta 35 do switch B	35	ISL de 100GbE para switch A porta 35
36	ISL de 100GbE para a porta 36 do switch B	36	ISL de 100GbE para switch A porta 36

Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você pode ["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 ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#) .
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) . Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando o...	Então...
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 9336C-FX2 e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp"](#). Caso contrário, acesse ["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 ter o seguinte:

- O kit de painel pass-through, disponível na NetApp (número da peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
- Para cada interruptor, oito parafusos 10-32 ou 12-24 e porcas de encaixe para montar os suportes e trilhos deslizantes nos postes dianteiros e traseiros do gabinete.
- O kit de trilho padrão da Cisco para instalar o switch em um gabinete NetApp .



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

- Para requisitos de preparação inicial, conteúdo do kit e precauções de segurança, consulte o ["Guia de Instalação de Hardware da Série Cisco Nexus 9000"](#).

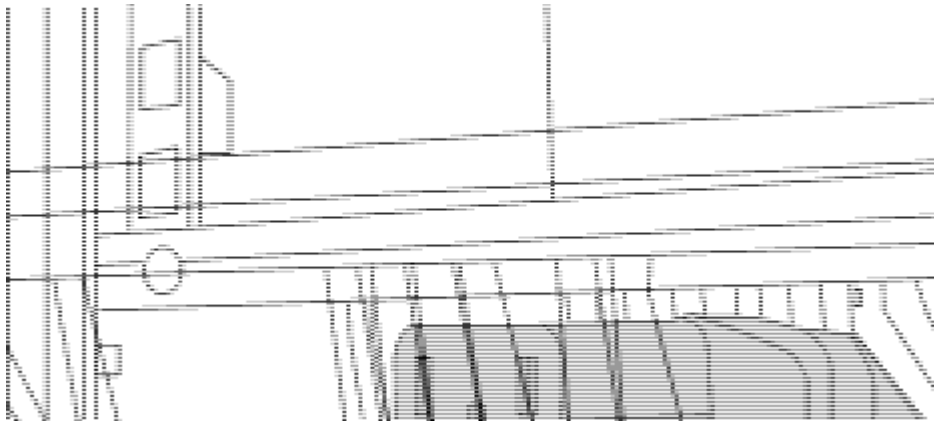
Passos

1. Instale o painel de vedação de passagem no gabinete NetApp .

- a. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego é instalado em U40.

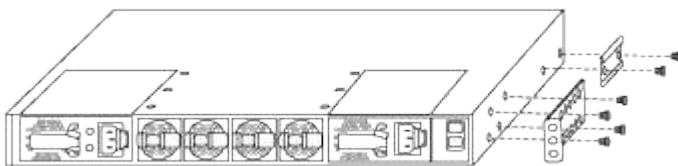
- b. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
- c. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
- d. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.



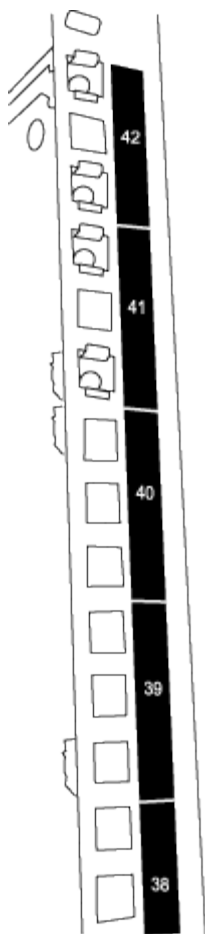
(1) Conector fêmea do cabo jumper.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.

- a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.



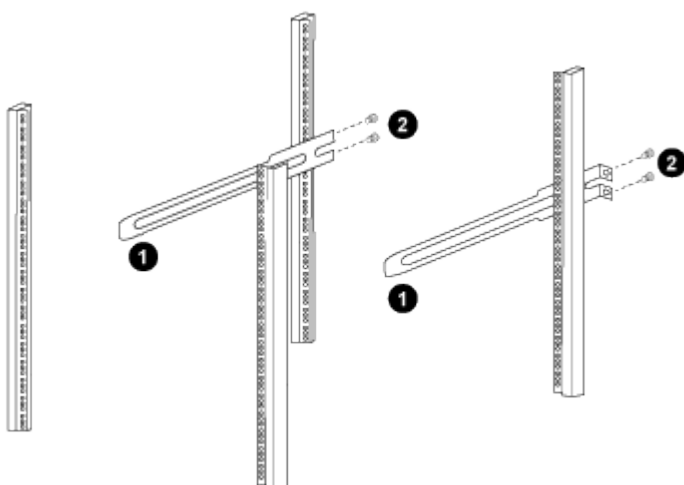
- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
3. Instale as porcas de clipe nos locais dos furos quadrados para todos 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 armário.

- a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os com os dedos.



(1) Ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos na cremalheira.

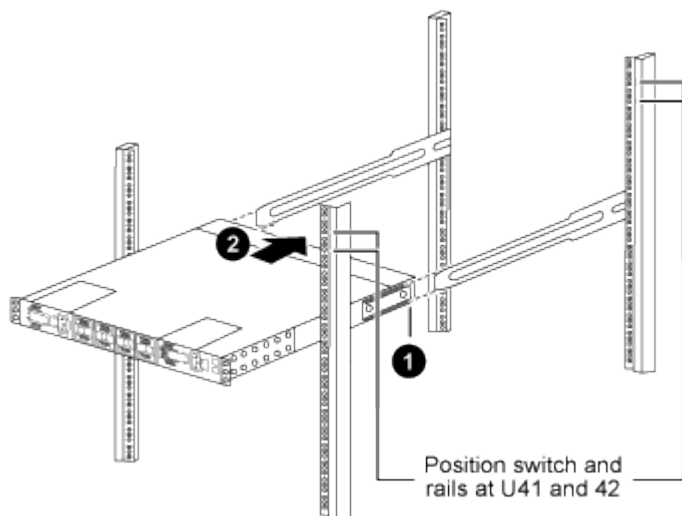
(2) Aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

- a. Repita o passo 4a para o poste traseiro do lado direito.
 - b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.
5. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

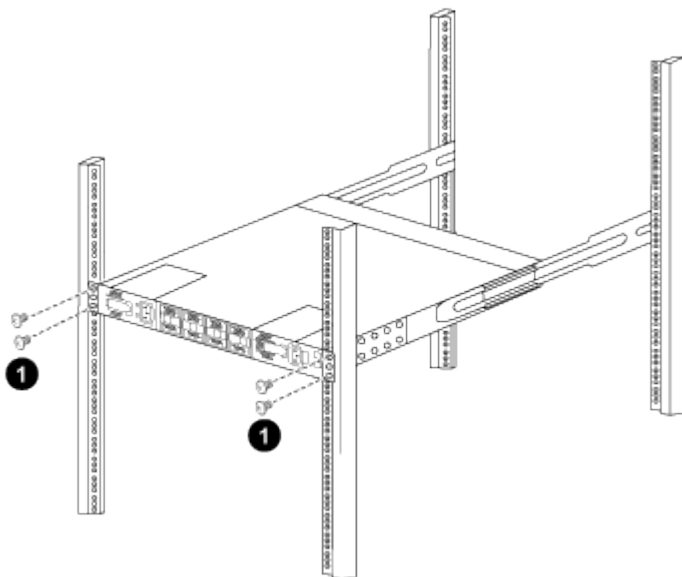
- a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

- b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

- a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos postes.
- b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

6. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
7. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

O que vem a seguir?

Após instalar os switches no gabinete NetApp, você pode [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 Ethernet NVIDIA CX6, CX6-DX e CX7.

Ao conectar uma porta de switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir a velocidade da porta do switch manualmente.

```
(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 de switch. Consulte o ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais

informações sobre os requisitos de instalação do switch.

Requisitos de FEC de 25GbE

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 comutação e0a e e0b, a configuração fec está 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 conectam 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 Knowledge Base ["As portas não se conectam no Cisco Nexus 9336C-FX2 devido a recursos TCAM."](#) para obter detalhes sobre como resolver esse 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 interruptor"

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 SSH"

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

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 ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#) .
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) . Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Realize uma configuração inicial dos switches de rede do cluster.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.

Incitar	Resposta
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	Digite o nome do interruptor, que está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave, de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.

Incitar	Resposta
Configurar camada de interface padrão (L3/L2)	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado)	Responda com noshut . O padrão é noshut.
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso)	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
3. Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software compatível com a NetApp para os switches a partir do ["Download do software Cisco"](#) página.

O que vem a seguir?

Depois de configurar seus switches, você pode ["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 Arquivo de Configuração de Referência (RCF), siga este procedimento.

Documentação sugerida

- ["Página do switch Ethernet da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornece informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são cluster1-01 e cluster1-02.
- Os nomes LIF dos clusters são cluster1-01_clus1 e cluster1-01_clus2 para o cluster1-01 e cluster1-02_clus1 e cluster1-02_clus2 para o cluster1-02.
- O `cluster1::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(`*>`) aparece.

3. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 do 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
```

Health					Speed (Mbps)	
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
```

Health					Speed (Mbps)	
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
```

Current Vserver Port	Home	Logical Current Is Interface	Status Admin/Oper	Network Address/Mask	Node

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 do cluster remoto:

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

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

```

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				

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

549

```

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. **[[passo 6]]** Verifique se o comando de reversão automática está habilitado 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
```

Vserver	Logical 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 vem a seguir?

Após preparar a instalação do software NX-OS e do RCF, você pode ["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."](#) .

Requisitos de revisão

Antes de começar

Certifique-se de fazer o seguinte:

- Execute o `show install all impact nxos bootflash:<image_name>.bin` comando no switch para revisar o impacto da instalação ou atualização da nova imagem do software NX-OS. Ele verifica a integridade da imagem, verifica se são necessárias reinicializações, avalia a compatibilidade do hardware e confirma se há espaço suficiente.
- Revise as notas de lançamento da versão de software NX-OS de destino para verificar se há algum requisito específico.
- Verifique se você possui um backup atual da configuração do switch.
- Verifique se você possui um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).

Documentação sugerida

- ["Página do switch Ethernet da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornecer informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF dos clusters 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::*>` O prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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. Exibir as portas do cluster em cada nó que estão conectadas 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
          e0b    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0b    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 do cluster.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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					
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

Health	Health				Speed (Mbps)	
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 principal:

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

Mostrar exemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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			
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 do software NX-OS em execução:

```
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 do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

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 após a reinicialização do switch:

```
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 reinicialize o switch. Se você estiver usando NX-OS 10.5(3)F ou posterior, não é necessário realizar uma atualização separada da imagem EPLD porque a imagem EPLD está incluída na imagem NX-OS. Ignore esta etapa e continue com a verificação da integridade da porta do cluster.

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 all
```

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 do cluster.

- a. Verifique se as portas do cluster estão ativas e funcionando corretamente 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	Broadcast	Domain	Link	MTU	Admin/Oper							
Port	IPspace												
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	Broadcast	Domain	Link	MTU	Admin/Oper							
Port	IPspace												
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	Broadcast	Domain	Link	MTU	Admin/Oper							
Port	IPspace												
Status	Status												

e0a	Cluster	Cluster		up	9000	auto/100000							
healthy	false												
e0b	Cluster	Cluster		up	9000	auto/100000							
healthy	false												

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)	
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.

b. Verifique o estado de saúde do switch no cluster.

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0b	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 Model	Type	Address	

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 poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.

```

13. Verifique se o cluster está íntegro:

```
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 switch cs1.

15. Verifique a conectividade das interfaces do cluster remoto antes de ativar a reversão automática nas LIFs do cluster:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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. Ative a reversão automática nos LIFs do cluster.

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

2. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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	e0b	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	e0b	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	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 alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que vem a seguir?

Após instalar ou atualizar o software NX-OS, você pode [instalar ou atualizar o arquivo de configuração de referência \(RCF\)](#).

Instale ou atualize o RCF

Visão geral da instalação ou atualização do Arquivo 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 Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configurações RCF disponíveis

A tabela a seguir descreve os RCFs disponíveis para diferentes configurações. Escolha o RCF aplicável à sua configuração. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

Configuração RCF	Descrição
2-Cluster-HA-Breakout	Suporta dois clusters ONTAP com pelo menos oito nós, incluindo nós que usam portas Cluster+HA compartilhadas.
4-Cluster-HA-Breakout	Suporta quatro clusters ONTAP com pelo menos quatro nós, incluindo nós que usam portas Cluster+HA compartilhadas.
1-Cluster-HA	Todas as portas estão configuradas para 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas. Requerido para os sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
1-Cluster-HA-Breakout	As portas estão configuradas para breakout 4x10GbE, breakout 4x25GbE (RCF 1.6+ em switches 100GbE) e 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas para nós que utilizam portas compartilhadas de cluster/HA: sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
Armazenamento de alta disponibilidade em cluster	As portas estão configuradas para 40/100GbE para Cluster+HA, 4x10GbE breakout para Cluster e 4x25GbE breakout para Cluster+HA, e 100GbE para cada par de armazenamento HA.
Conjunto	Duas versões do RCF com diferentes alocações de portas 4x10GbE (breakout) e portas 40/100GbE. Todos os nós FAS/ AFF são suportados, exceto os sistemas AFF A320, AFF A250 e FAS500f .
Armazenar	Todas as portas estão configuradas para conexões de armazenamento NVMe de 100GbE.

RCFs disponíveis

A tabela a seguir lista os RCFs disponíveis para os switches 9336C-FX2 e 9336C-FX2-T. Escolha a versão do RCF aplicável para sua configuração. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

Nome da RCF
Cluster-HA-Breakout RCF 1.xx
Cluster-HA-Storage RCF 1.xx

Nome da RCF
Armazenamento RCF 1.xx
MultiCluster-HA RCF 1.xx

Documentação sugerida

- ["Switches Ethernet Cisco \(NSS\)"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 9000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF dos clusters 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::*>` O prompt indica o nome do cluster.

Os exemplos neste procedimento utilizam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE, **e0a** e **e0b**. Consulte a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Para obter detalhes sobre as configurações RCF disponíveis, consulte o ["fluxo de trabalho de instalação de software"](#).

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

O que vem a seguir?

Após revisar o procedimento de instalação ou atualização do RCF, você pode ["instalar o RCF"](#) ou ["atualize seu RCF"](#) Conforme necessário.

Instale o arquivo 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 conexão de console com o switch. A conexão com o console é opcional se você tiver acesso remoto ao switch.
- Os switches cs1 e cs2 estão ligados e a configuração inicial dos switches está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão desejada do NX-OS foi instalada.
- As conexões ISL entre os switches estão conectadas.
- As portas do cluster de nós ONTAP não estão conectadas.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch cs1 usando SSH ou usando um console serial.
2. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

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 do show banner motd comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas 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
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.
7. Após verificar se as versões do 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 de configuração em `write_erase.cfg` arquivo no bootflash.

Certifique-se de configurar o seguinte:



- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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. Ao instalar o 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
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

10. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

11. Repita os passos 1 a 10 no switch cs2.

12. Conecte as portas de cluster de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```


Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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 sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

3. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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#
```

Etapa 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager oferece um fluxo de trabalho simples e fácil para a configuração e instalação de clusters, incluindo a atribuição de um endereço IP de gerenciamento de nó, a inicialização do cluster, a criação de uma camada local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Vá para ["Configurar o ONTAP em um novo cluster com o System Manager"](#) Para obter instruções de configuração.

O que vem a seguir?

Após instalar o RCF, você pode ["verificar a configuração SSH"](#).

Atualize seu Arquivo de Configuração de Referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapas 1: Prepare-se para a atualização

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

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

Onde x representa a duração do período de manutenção em horas.

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

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exibir as portas do cluster em cada nó que estão conectadas 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::*>
```

4. Verifique o status administrativo e operacional de cada porta do cluster.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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

Health	Health				Speed (Mbps)	
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 principal:

```
network interface show -vserver cluster
```

Mostrar exemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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::*>
```

5. 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, desligue as portas conectadas às portas de cluster dos nós.

```
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
```



Certifique-se de desligar **todas** as portas do cluster conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base "[Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional.](#)" para obter mais detalhes.

2. Verifique se as LIFs do cluster foram transferidas 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			

```
8 entries were displayed.  
cluster1::*>
```

3. Verifique se o cluster está íntegro:

```
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. Caso ainda não o tenha feito, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

```
show running-config
```

- Registre quaisquer adições personalizadas entre o atual `running-config` e o arquivo RCF em uso (como uma configuração SNMP para sua organização).
 - A partir do NX-OS 10.2, utilize o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, use uma ferramenta de comparação/diferenciação de terceiros.
5. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
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. Ao atualizar para a versão 1.12 ou posterior do RCF, 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
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

7. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Execute o comando `write erase` para apagar a configuração salva atualmente:

```
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 para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Execute um reinício do switch:

```
switch# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

11. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

12. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de](#)

Comandos do Cisco Nexus Série 9000 NX-OS".

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
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

14. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

15. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração.](#)" Para obter detalhes sobre quaisquer alterações adicionais necessárias.
16. Após verificar se as versões do RCF, as adições personalizadas e as configurações de interruptores estão corretas, copie o arquivo `running-config` para o arquivo `startup-config`.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na "[Guia de Comandos do Cisco Nexus Série 9000 NX-OS](#)".

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

17. Reinicie o interruptor cs1. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e os eventos de "portas de cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

18. Verifique a integridade das portas do cluster.

- a. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

```
network port show -ip space cluster
```

Mostrar exemplo

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

Node: cluster1-01

Ignore

						Speed (Mbps)
Health	Health	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
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	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
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	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)	
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 o estado de saúde do switch no cluster.

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Model	Type	Address	
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 poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.

```

19. Verifique se o cluster está íntegro:

```
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::*>

```

20. Repita os passos 1 a 19 no switch cs2.

21. Ative a reversão automática nos LIFs do cluster.

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

22. Execute uma reinicialização do switch cs2.

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

Etapa 3: Verifique a configuração de rede do cluster e a integridade do cluster.

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 conectados:

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. Verifique se os nós do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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 sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

4. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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		
8 entries were displayed.				
cluster1::*>				

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver vservice_name -lif lif_name
```

6. Verifique se o cluster está íntegro:

```
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 do cluster remoto:

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

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

```

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				

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

609

```

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 vem a seguir?

Após atualizar seu RCF, você pode ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de

coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches do 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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIAbm1zdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer          1          enabled
(switch)#
```



Ao habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Consulte ["Configure a segurança de rede usando FIPS."](#) para mais detalhes.

O que vem a seguir?

Após verificar sua configuração SSH, você pode ["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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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.

O que vem a seguir

Depois de reiniciar os interruptores, você pode [reconfigurar](#) eles conforme necessário.

Migre 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.

Requisitos de revisão

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.

Interruptores 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"](#). Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

O que você vai precisar

Verifique se sua configuração atende aos seguintes requisitos:

- O cluster existente está configurado corretamente e funcionando.
- Todas as portas do cluster estão no estado **ativo** para garantir operações sem interrupções.
- 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 do cluster existente apresenta as seguintes características:
 - Um cluster NetApp redundante e totalmente funcional, utilizando switches NetApp CN1610.
 - Conectividade de gerenciamento e acesso ao console tanto para os switches NetApp CN1610 quanto para os novos switches.
 - Todas as LIFs do cluster estão ativas e conectadas às suas portas de origem.
- 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.

Migre os switches

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os switches de cluster CN1610 existentes são *C1* e *C2*.
- Os novos interruptores de cluster 9336C-FX2 são *cs1* e *cs2*.
- Os nós são *node1* e *node2*.
- Os LIFs do cluster são *node1_clus1* e *node1_clus2* no nó 1, e *node2_clus1* e *node2_clus2* no nó 2, respectivamente.
- O `cluster1::*>` O 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 interruptor C2 é substituído primeiro pelo interruptor cs2.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Todas as LIFs do cluster fazem failover para o novo switch cs2.
 - Em seguida, o cabeamento entre os nós e o C2 é desconectado do C2 e reconectado ao cs2.
- O interruptor C1 é substituído pelo interruptor cs1.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Todas as LIFs do cluster fazem failover para o novo switch cs1.
 - Em seguida, o cabeamento entre os nós e C1 é desconectado de C1 e reconectado a cs1.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir transfere todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Etapa 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Desative a reversão automática nos LIFs do cluster.

Ao desativar a reversão automática para este procedimento, as LIFs do cluster não retornarão automaticamente à sua porta original. Eles permanecem no porto atual enquanto ele continuar funcionando.

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

Etapa 2: Configurar portas e cabos

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

Cada porta deve aparecer para cima. `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

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Exibir informações sobre os LIFs e seus respectivos nós de origem:

```
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
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 do cluster em cada nó são conectadas aos switches de cluster existentes da seguinte maneira (da perspectiva dos nós), utilizando 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 switches do cluster estão conectados da seguinte forma (do ponto de vista 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
C2 0/13	0/13	179	S I s	CN1610
C2 0/14	0/14	175	S I s	CN1610
C2 0/15	0/15	179	S I s	CN1610
C2 0/16	0/16	175	S I s	CN1610

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
C1 0/13	0/13	175	S I s	CN1610
C1 0/14	0/14	175	S I s	CN1610
C1 0/15	0/15	175	S I s	CN1610
C1 0/16	0/16	175	S I s	CN1610

4. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 5]] No switch C2, desligue as portas conectadas às portas do cluster dos nós para realizar o failover das LIFs do cluster.



Não tente migrar manualmente os 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

```

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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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
```

Current Is	Logical	Status	Network	Current
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, desligue as portas conectadas às portas do cluster dos nós para realizar o 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 exibir 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 possuem uma conexão com cada switch:

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


Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 reversão automática nos LIFs do cluster:

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

2. No switch cs2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

3. Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verifique se o cluster está íntegro:

```
cluster show
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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
```

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 6]]Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["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.

Requisitos de revisão

Assegure-se de que:

- Você verificou o número de série do switch para garantir que o switch correto seja migrado.

- Algumas portas dos switches Nexus 9336C-FX2 são configuradas para operar em 10GbE ou 40GbE.
- A conectividade de 10GbE e 40GbE dos nós aos switches de cluster Nexus 9336C-FX2 foi planejada, migrada e documentada.
- O cluster está funcionando perfeitamente (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 de software recomendada mais recente.
 - Confirme se os Arquivos de Configuração de Referência (RCFs) foram totalmente aplicados a todos os novos switches antes de migrar as LIFs para eles.
 - Verifique as configurações de funcionamento e inicialização em ambos os switches antes de redirecionar o tráfego de rede.
 - Qualquer personalização do site, como DNS, NTP, SMTP, SNMP e SSH, é configurada nos novos switches.
- Você tem acesso à tabela de compatibilidade de switches em ["Switches Ethernet da Cisco"](#) Página com as versões suportadas do ONTAP, NX-OS e RCF.
- Você já consultou os guias de software e atualização apropriados disponíveis no site da Cisco para os procedimentos de atualização e downgrade do switch Cisco ? ["Suporte para switches Cisco Nexus série 9000"](#) página.



Se você estiver alterando a velocidade das portas de cluster e0a e e1a nos sistemas AFF A800 ou AFF C800 , poderá observar o recebimento de pacotes malformados após a conversão de velocidade. Ver ["Erro 1570339"](#) e o artigo da Base de Conhecimento ["Erros de CRC em portas T6 após conversão de 40GbE para 100GbE"](#) para orientação.

Migre os switches

Sobre os exemplos

Os exemplos neste procedimento utilizam dois nós. Esses nós utilizam duas portas de interconexão de cluster 10GbE, e0a e e0b. Veja o ["Hardware Universe"](#) Para verificar as portas de cluster corretas em suas plataformas. Ver ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) Para obter mais informações sobre os requisitos de instalação do switch.

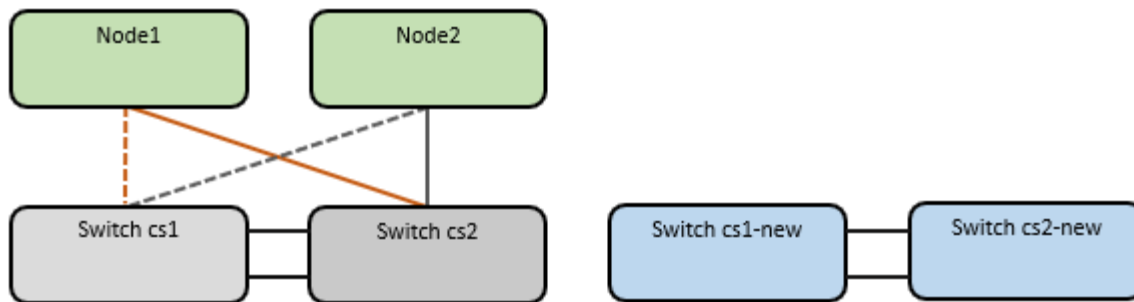


Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco existentes são **cs1** e **cs2**.
- Os novos switches de cluster Nexus 9336C-FX2 são **cs1-new** e **cs2-new**.
- Os nomes dos nós são **node1** e **node2**.
- Os nomes 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 ONTAP e "[Switches da série Nexus 9000](#)". Os comandos utilizados são os comandos ONTAP, salvo indicação em contrário.

Este procedimento abrange o seguinte cenário:

- Switch cs2 é substituído primeiro por switch cs2-new.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Todas as LIFs do cluster fazem failover para o novo switch cs2-new.
 - A fiação entre os nós e o cs2 é então desconectada do cs2 e reconectada ao cs2-new.
- O switch cs1 foi substituído pelo switch cs1-new.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Todas as LIFs do cluster fazem failover para o novo switch cs1-new.
 - A fiação entre os nós e o cs1 é então desconectada do cs1 e reconectada ao cs1-new.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir transfere todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Etapa 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

Etapas 2: Configurar portas e cabos

1. Nos novos switches, confirme se o cabo ISL está conectado e funcionando corretamente entre os switches cs1-new e cs2-new:

```
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. Exibir as portas do cluster em cada nó que estão conectadas aos switches de 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

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

Mostrar exemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

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

```
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 Model	Type	Address	
cs1 C5596UP	cluster-network	10.233.205.92	N5K-
Serial Number: FOXXXXXXXXGS			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version			
9.3(4)			
Version Source: CDP			
cs2 C5596UP	cluster-network	10.233.205.93	N5K-
Serial Number: FOXXXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version			
9.3(4)			
Version Source: CDP			

4. Desative a reversão automática nos LIFs do cluster.

Ao desativar a reversão automática para este procedimento, as LIFs do cluster não retornarão automaticamente à sua porta original. Eles permanecem no porto atual enquanto ele continuar funcionando.

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



Desativar a reversão automática garante que o ONTAP só realize o failover das LIFs do cluster quando as portas do switch forem desligadas posteriormente.

5. No switch de cluster cs2, desligue as portas conectadas às portas de cluster de **todos** os nós para realizar o failover das LIFs do 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 do cluster foram transferidas 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 íntegro:

```
cluster show
```

Mostrar exemplo

```

cluster1::*> cluster show

```

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

8. Se as LIFs do cluster tiverem migrado para o switch cs1 e o cluster estiver íntegro, acesse [Etapa. 10](#) . Se algumas LIFs do cluster não estiverem íntegras ou se o cluster estiver com problemas, você pode reverter a conectividade com o switch cs2, da seguinte forma:

- a. Ative as portas conectadas às portas do 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 do cluster foram transferidas 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 íntegro:

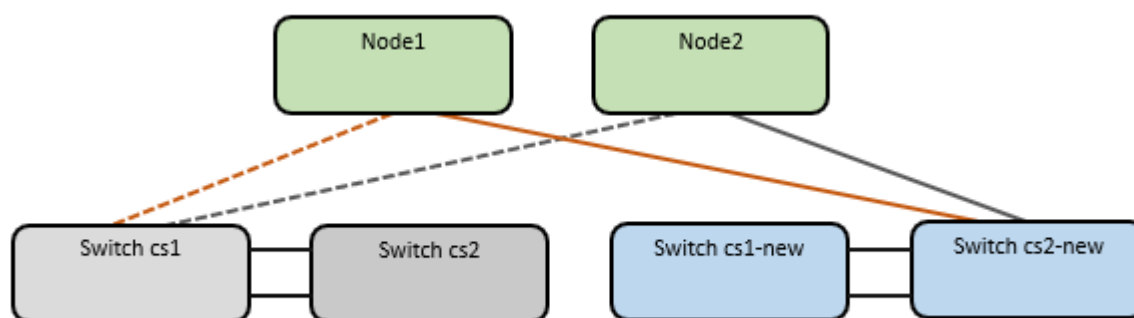
```
cluster show
```

Mostrar exemplo

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

9. Após restaurar o LIF e a integridade do cluster, reinicie o processo a partir de [Etapa. 4](#).
10. Mova todos os cabos de conexão do nó do cluster do switch cs2 antigo para o novo switch cs2-new.

Cabos de conexão do nó do cluster movidos para o switch cs2-new



11. Confirme a integridade das conexões de rede migradas 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 do cluster que foram movidas devem estar ativas.

12. Verifique as informações dos vizinhos nas portas do cluster:

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


Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol	Local Port	Discovered 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 enxergam o switch cs2-new como vizinho.

13. Confirme as conexões das portas do switch a partir da perspectiva do switch cs2-new:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. No switch de cluster cs1, desligue as portas conectadas às portas de cluster de **todos** os nós para realizar o failover das LIFs do 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 do cluster são transferidas para o switch cs2-new em caso de falha.

15. Verifique se as LIFs do cluster foram transferidas para as portas hospedadas no switch cs2-new. 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 íntegro:

```
cluster show
```

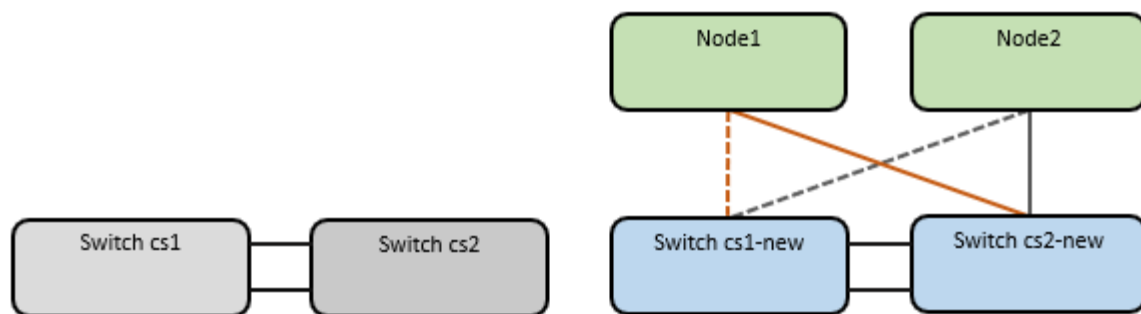
Mostrar exemplo

```
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 cs1-new.

Cabos de conexão do nó do cluster movidos para o switch cs1-new



18. Confirme a integridade das conexões de rede migradas 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 do cluster que foram movidas devem estar ativas.

19. Verifique as informações dos vizinhos 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 enxergam o switch cs1-new como vizinho.

20. Confirme as conexões das portas do switch a partir da perspectiva do switch cs1-new:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

21. Verifique se o ISL entre cs1-new e cs2-new 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. No switch cs2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

3. Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verifique se o cluster está íntegro:

```
cluster show
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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
```

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 6]]Se você desativou a criação automática de casos, reative-a invocando uma mensagem do `AutoSupport:system node autosupport invoke -node * -type all -message MAINT=END`

O que vem a seguir?

Depois de migrar os switches, você pode [configurar monitoramento de integridade do switch](#) .

Migrar para um 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 utilizam portas ópticas ou Twinax, mas não é suportado neste switch se os nós estiverem utilizando portas RJ45 10Gb BASE-T integradas para as portas de rede do cluster.

Requisitos de revisão

O que você vai precisar

- Para a configuração sem switch de dois nós:
 - A configuração sem switch de dois nós está configurada corretamente e funcionando.

- Todas as portas do cluster estão no estado **ativo**.
- Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e em suas portas de origem.
- Consulte a "[Hardware Universe](#)" para todas as versões do ONTAP compatíveis.
- Para a configuração do switch Cisco Nexus 9336C-FX2:
 - Ambos os switches possuem conectividade de rede de gerenciamento.
 - É possível acessar os switches do cluster através do console.
 - As conexões nó a nó e switch a switch do Nexus 9336C-FX2 usam cabos Twinax ou de fibra.

Consulte o "[Hardware Universe](#)" para obter mais informações sobre cabeamento.

- Os cabos Inter-Switch Link (ISL) são conectados às portas 1/35 e 1/36 em ambos os switches 9336C-FX2.
- A personalização inicial dos dois switches 9336C-FX2 foi 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 do site, como SMTP, SNMP e SSH, é configurada nos novos switches.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- 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, respectivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas do cluster utilizadas neste procedimento são e0a e e0b.

Consulte a "[Hardware Universe](#)" para obter informações sobre as portas de cluster para suas plataformas. Consulte "[Que informações adicionais preciso para instalar meu equipamento que não está no HWU?](#)" para obter mais informações sobre os requisitos de instalação do switch.

Migre os switches

Etapa 1: Prepare-se para a migração

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

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

Etapa 2: Configurar portas e cabos

1. Desative todas as portas voltadas para os nós (exceto as portas ISL) nos dois novos switches do cluster, cs1 e cs2.

Não desative as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra que as portas voltadas para o nó, de 1 a 34, 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 ativos nas portas 1/35 e 1/36:

```
show port-channel summary
```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão ativas no switch 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 ativas no switch 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 conectados 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 aparecer para cima. Link e saudável para Health Status .

Mostrar exemplo

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

Node: node1

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

Node: node2

Port	IPspace	Broadcast Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health 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 do cluster estão ativas e operacionais:

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

Cada LIF de cluster deve exibir true para Is Home e tenha um Status Admin/Oper de cima/para cima.

Mostrar exemplo

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

Current Is	Logical	Status	Network	Current
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. Desative a reversão automática em todas as LIFs do cluster:

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

Mostrar exemplo

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

Vserver	Logical	Auto-revert
Interface		

Cluster		
	node1_clus1	false
	node1_clus2	false
	node2_clus1	false
	node2_clus2	false
4 entries were displayed.		

7. Desconecte o cabo da porta do cluster e0a no nó 1 e, em seguida, conecte e0a à porta 1 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.

O "[Hardware Universe - Switches](#)" Contém mais informações sobre cabeamento.

- Desconecte o cabo da porta do cluster e0a no nó 2 e, em seguida, conecte e0a à porta 2 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
- Habilite todas as portas voltadas para os nós no switch de cluster cs1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão habilitadas 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
```

- Verifique se todas as LIFs do cluster estão ativas e operacionais:

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

Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs estão ativas no node1 e no node2:

```
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					

4 entries were displayed.

11. Exibir informações sobre o estado 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. Desconecte o cabo da porta do cluster e0b no nó 1 e, em seguida, conecte e0b à porta 1 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
13. Desconecte o cabo da porta do cluster e0b no nó 2 e, em seguida, conecte e0b à porta 2 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
14. Habilite todas as portas voltadas para os nós no switch de cluster cs2.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão habilitadas 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 ativas no nó 1 e no nó 2:

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

Node: node1

Ignore

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

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. Ative a reversão automática nos LIFs do cluster.

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

2. No switch cs2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

3. Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verifique se todas as interfaces exibem verdadeiro para Is Home :

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



Isso pode levar alguns minutos para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs estão ativas no nó 1 e no nó 2 e que Is Home Os resultados são verdadeiros:

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

Current Is	Logical	Status	Network	Current	
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 ambos os nós possuem uma conexão com cada switch:

```
show cdp neighbors
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
(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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs2 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs2 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	133	H	FAS2980
node2 e0b	Eth1/2	133	H	FAS2980
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

6. Exibir 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
           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.
```

7. Verifique se as configurações estão desativadas:

```
network options switchless-cluster show
```



A conclusão do comando pode levar alguns minutos. Aguarde o anúncio de que o tempo de vida de 3 minutos está prestes a expirar.

O resultado incorreto no exemplo a seguir mostra que as configurações estão desativadas:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

8. Verifique o status dos nós membros do cluster:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde e a elegibilidade dos nós no cluster:

```
cluster1::*> cluster show
```

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

9. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. **[[passo 10]]**Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["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).

Requisitos de revisão

Antes de substituir o interruptor, certifique-se de que:

- Você verificou o número de série do interruptor para garantir que o interruptor correto seja substituído.
- Na infraestrutura de cluster e rede existente:
 - O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
 - Todas as portas do cluster estão **ativas**.
 - Todas as interfaces lógicas do cluster (LIFs) estão **ativas** e em suas portas de origem.
 - O ONTAP `cluster ping-cluster -node node1` O comando deve indicar que a conectividade básica e a comunicação com dispositivos maiores que PMTU estão funcionando corretamente em todos os caminhos.
- No switch de substituição Nexus 9336C-FX2:
 - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - As conexões do nó são as portas 1/1 a 1/34.
 - Todas as portas Inter-Switch Link (ISL) estão desabilitadas nas portas 1/35 e 1/36.
 - O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional NX-OS são carregados no switch.
 - A personalização inicial do interruptor está concluída, conforme detalhado em ["Configurar o switch de cluster 9336C-FX2"](#).

Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, são copiadas para o novo switch.

- Você executou o comando para migrar uma LIF de cluster do nó onde a LIF de cluster está hospedada.

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster em cada nó são denominadas e0a e e0b.
- Os nomes 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 para alterações em todos os nós do cluster é cluster1::*>

Sobre esta tarefa

O procedimento a seguir baseia-se na seguinte topologia de rede em 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/Protocol	Local Port	Discovered 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
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2	Eth1/35	176	R S I s	N9K-C9336C	
cs2 (FD0220329V5)	Eth1/36	176	R S I s	N9K-C9336C	

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
```

Etapa 1: Prepare-se para a substituição

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

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Instale o RCF e a imagem apropriados no switch, newcs2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e NX-OS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e NX-OS, continue para a etapa 2.

- a. Acesse a página *NetApp Cluster and Management Network Switches Reference Configuration File Description* no site de suporte da NetApp .
 - b. Clique no link para a *Matriz de Compatibilidade de Rede de Cluster e Rede de Gerenciamento* e, em seguida, observe a versão de software do switch necessária.
 - c. Clique na seta "Voltar" do seu navegador para retornar à página de Descrição, clique em **CONTINUAR**, aceite o contrato de licença e, em seguida, acesse a página de Download.
 - d. Siga os passos na página de Download para baixar os arquivos RCF e NX-OS corretos para a versão do software ONTAP que você está instalando.
3. No novo switch, efetue login como administrador e desligue todas as portas que serão conectadas às interfaces do cluster de nós (portas 1/1 a 1/34).

Se o interruptor que você está substituindo não estiver funcionando e estiver desligado, vá para a Etapa 4. As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em 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
```

Vserver	Logical 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todas as versões do ONTAP

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

```
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 conecte-os às mesmas portas no switch Nexus C9336C-FX2 newcs2.
3. Abra as portas ISLs 1/35 e 1/36 entre os switches cs1 e newcs2 e, em seguida, verifique o status da operação do canal da porta.

Port-Channel deve indicar Po1(SU) e Member Ports deve indicar Eth1/35(P) e Eth1/36(P).

Mostrar exemplo

Este exemplo habilita as portas ISL 1/35 e 1/36 e exibe o resumo do canal de porta no switch 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

O resultado deverá ser semelhante ao seguinte:

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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 a LIF do cluster associada à porta da etapa anterior usando o comando `network interface revert`.

Mostrar exemplo

Neste exemplo, a LIF node1_clus2 no nó 1 é revertida com sucesso se o valor de Home for verdadeiro e a porta for e0b.

Os seguintes comandos retornam LIF node1_clus2 sobre node1 para o porto de origem e0a e exibe informações sobre os LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se a coluna "Is Home" (É o nó principal) for verdadeira para ambas as interfaces do cluster e elas mostrarem as atribuições de porta corretas, neste exemplo. e0a e e0b no nó 1.

```
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 o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

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

7. Verifique se todas as portas físicas do cluster estão ativas:

```
network port show ipspace Cluster
```

Mostrar exemplo

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

Node node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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 do 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C

```
Total entries displayed: 4
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["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 uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

Requisitos de revisão

Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

Antes de começar

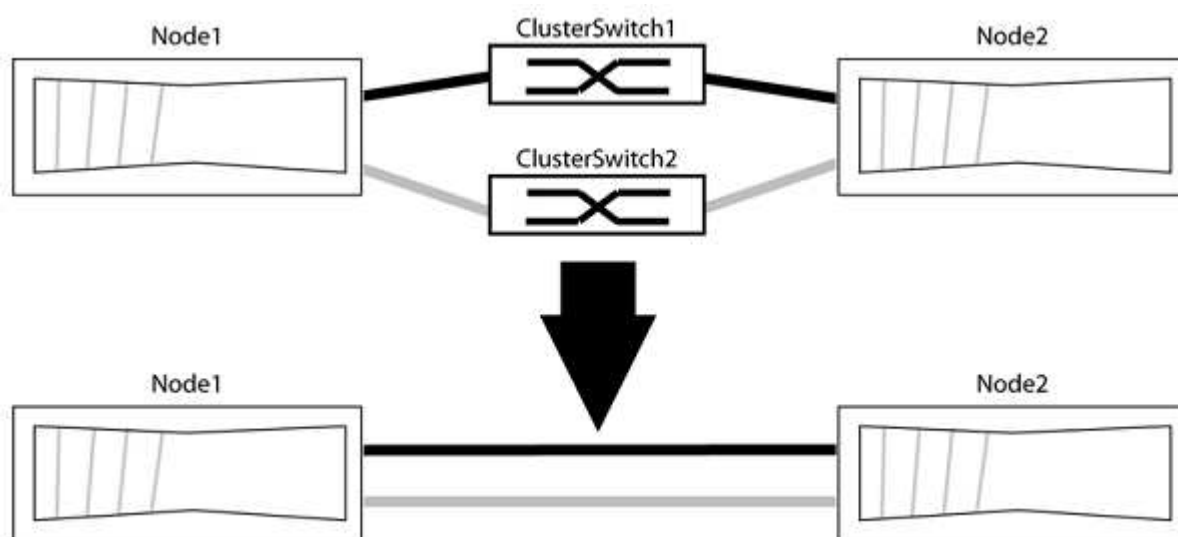
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migre 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 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 elas variam de acordo com o sistema.

Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

onde `h` é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

Mostrar exemplo

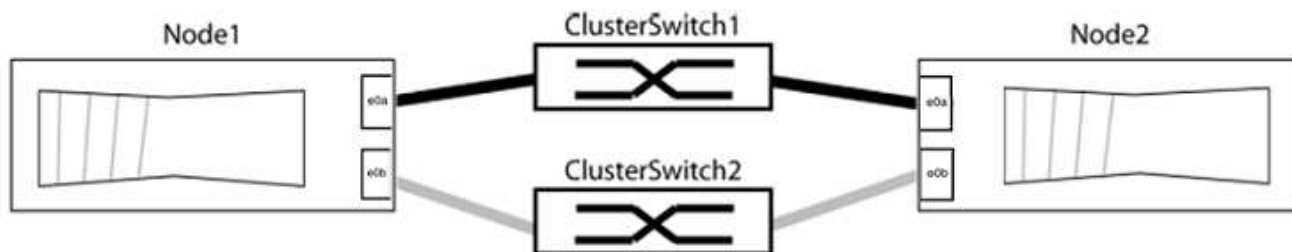
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de up para a coluna “Link” e um valor de healthy para a coluna “Estado de Saúde”.

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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está true para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

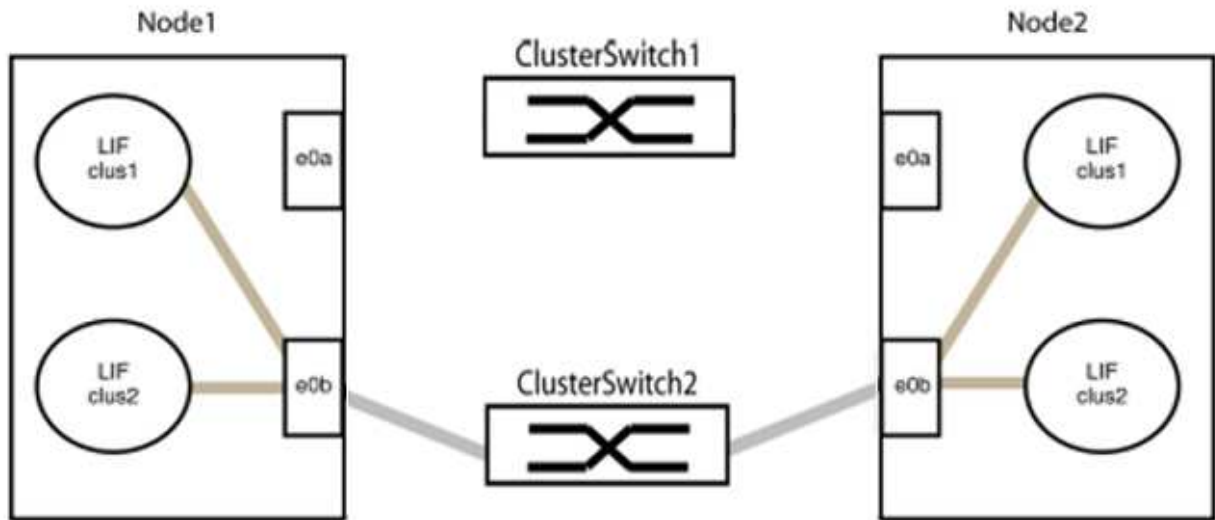
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

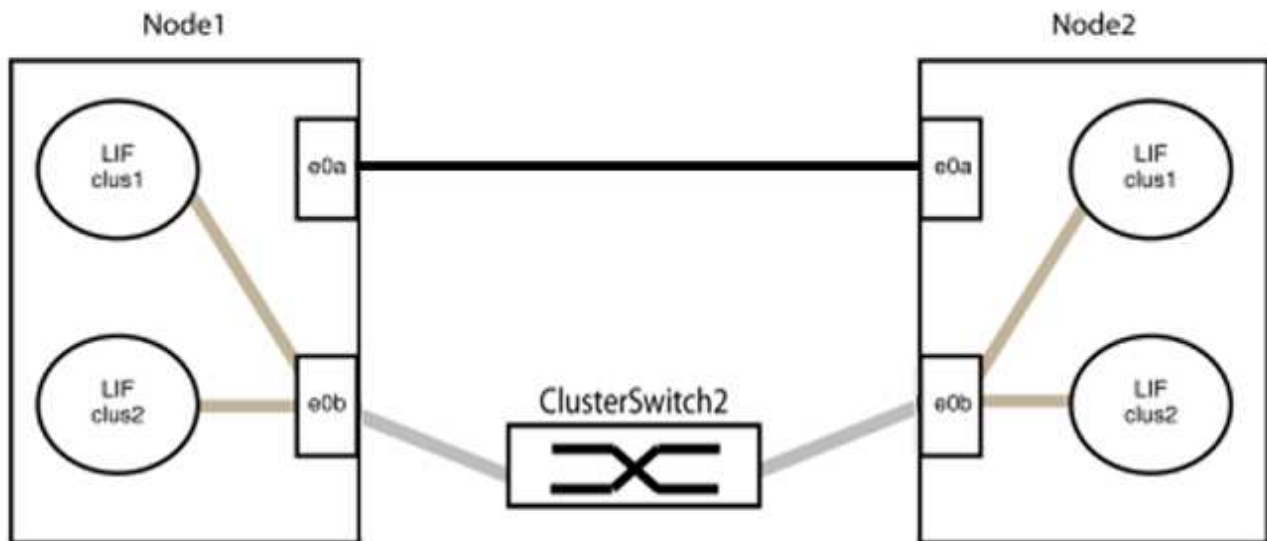
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

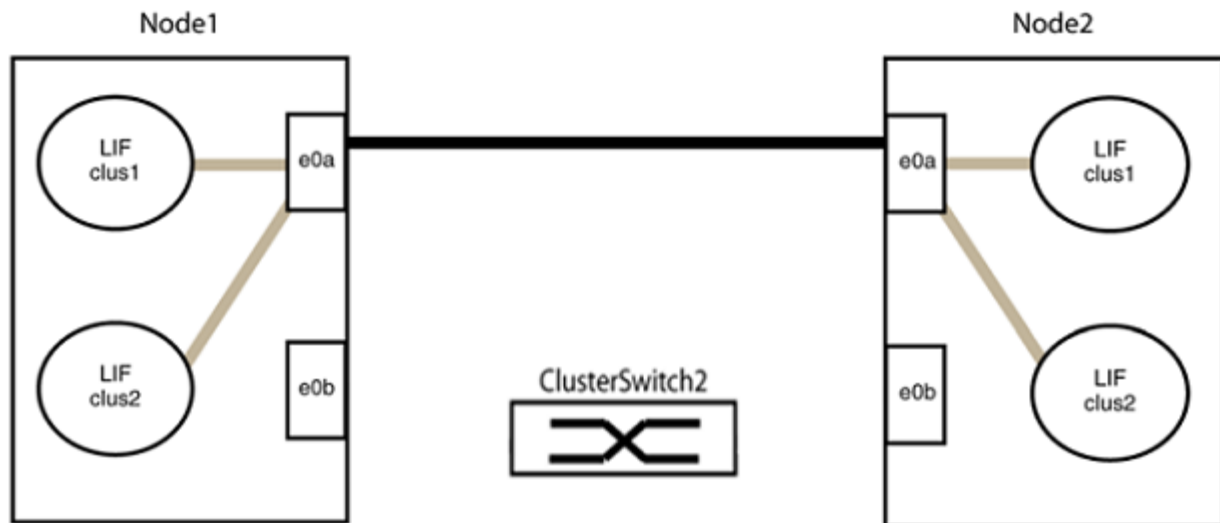
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

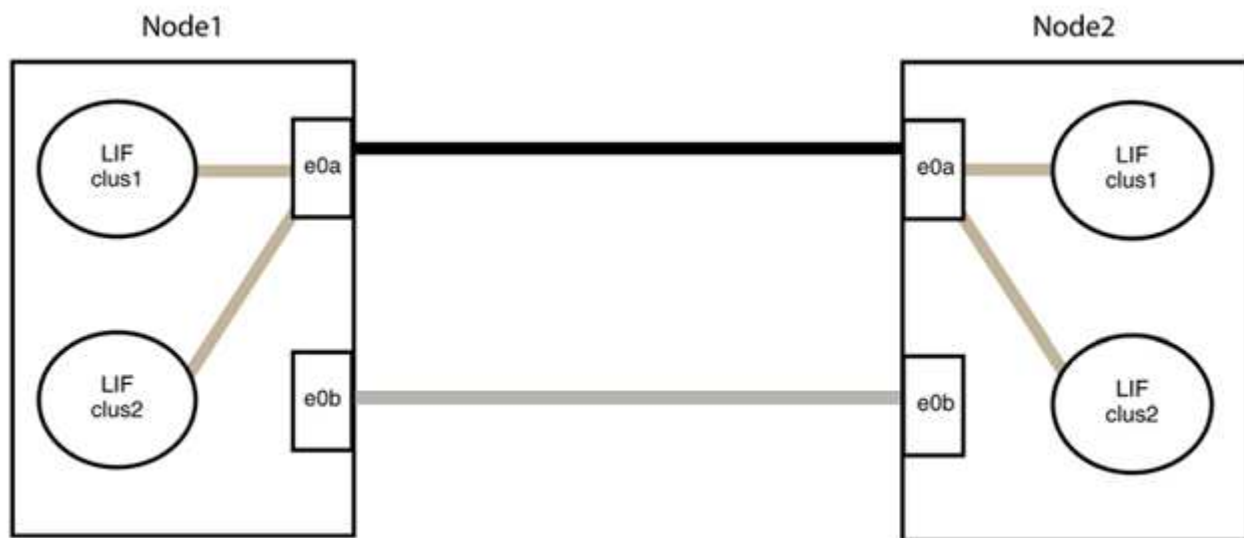
- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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
    e0b      node2
node1/lldp
    e0a      node2 (00:a0:98:da:16:44)
    e0b      node2 (00:a0:98:da:16:44)
node2/cdp
    e0a      node1
    e0b      node1
node2/lldp
    e0a      node1 (00:a0:98:da:87:49)
    e0b      node1 (00:a0:98:da:87:49)
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 valores de LIF foram revertidos se a coluna “Is Home” estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 6]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

NVIDIA SN2100

Começar

Fluxo de trabalho de instalação e configuração para switches NVIDIA SN2100

O NVIDIA SN2100 é um switch de cluster que permite criar clusters 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 instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar todos os requisitos de configuração.

Requisitos de instalação

Se você deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar interruptores de gerenciamento adicionais, que são opcionais.

Você instala o switch NVIDIA SN2100 (X190006) no gabinete de switch duplo/simples da NVIDIA com os suportes padrão que acompanham o switch.

Para diretrizes de cabeamento, consulte ["Analise as considerações sobre cabeamento e configuração."](#)

Suporte para ONTAP e Linux

O switch NVIDIA SN2100 é um switch 10/25/40/100GbE que executa o Cumulus Linux. O switch suporta o seguinte:

- ONTAP 9.10.1P3 e versões posteriores

O switch SN2100 atende a aplicações de Cluster e Armazenamento no ONTAP 9.10.1P3 e versões posteriores em diferentes pares de switches.

- Versões do sistema operacional Cumulus Linux (CL)

- Versões CL específicas são qualificadas e suportadas por NetApp. Para obter informações de compatibilidade atuais, consulte ["Informações sobre switches Ethernet da NVIDIA"](#) ou o ["Hardware Universe"](#).
- Para baixar o software SN2100 Cumulus da NVIDIA, você precisa ter credenciais de login para acessar o Portal de Suporte Empresarial da NVIDIA. Consulte o artigo da Knowledge Base ["Como se cadastrar no Portal de Suporte Empresarial da NVIDIA para obter acesso."](#).
- Você pode instalar o Cumulus Linux quando o switch estiver executando o Cumulus Linux ou o ONIE.

O que vem a seguir?

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

Componentes e números de peça para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de consultar a lista de componentes e os números de peça do gabinete e do kit de trilhos.

Detalhes do gabinete

Você instala o switch NVIDIA SN2100 (X190006) no gabinete de switch duplo/simples da NVIDIA com os suportes padrão que acompanham o switch.

Detalhes do kit de trilhos

A tabela a seguir lista o número da peça e a descrição dos interruptores e kits de trilhos SN2100:

Número da peça	Descrição
X190006-PE	Cluster Switch, NVIDIA SN2100, 16PT 100GbE, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16PT 100GbE, PSIN
X-MTEF-KIT-D	Kit de trilhos, interruptor duplo NVIDIA lado a lado
X-MTEF-KIT-E	Kit de trilhos, NVIDIA Single Switch de profundidade reduzida



Consulte a documentação da NVIDIA para obter detalhes sobre ["Instalando seu kit de trilhos e interruptor SN2100"](#).

O que vem a seguir?

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches NVIDIA SN2100

Para a instalação do switch NVIDIA SN2100, certifique-se de revisar toda a documentação recomendada.

Título	Descrição
"Guia de Instalação do NVIDIA Switch"	Este guia descreve como instalar seus switches NVIDIA SN2100.
"Guia de cabeamento para gaveta de unidades NVMe NS224"	Visão geral e ilustrações mostrando como configurar a cablagem para gavetas de unidades de disco.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Permite que você confirme o hardware compatível, como switches de cluster 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."](#)

Analise os requisitos para conexões ópticas, o adaptador QSA e a velocidade da porta do switch.

3

["Conecte os cabos às prateleiras NS224."](#)

Siga os procedimentos de cabeamento se você tiver um sistema no qual os gabinetes de unidades NS224 precisam ser cabeados como armazenamento conectado ao switch (e não como armazenamento conectado diretamente).

Instale o hardware para o switch NVIDIA SN2100.

A instalação do hardware do switch NVIDIA SN2100 é um primeiro passo crucial na construção de uma infraestrutura de rede confiável e escalável para suportar fluxos de trabalho de proteção, replicação e gerenciamento de dados.

Siga estas etapas para configurar seus switches SN2100. Consulte a documentação da NVIDIA para obter instruções detalhadas.

Passos

- 1. Analise o ["requisitos de configuração"](#) .
- 2. Siga as instruções no ["Guia de Instalação do NVIDIA Switch"](#).

O que vem a seguir?

Após instalar o hardware, você pode ["revisar cabeamento e configuração"](#) requisitos.

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seu switch NVIDIA SN2100, revise as seguintes considerações.

Detalhes da porta NVIDIA

Portas de comutação	Utilização de portas
swp1s0-3	Nós de porta de cluster breakout 4x10GbE
swp2s0-3	Nós de porta de cluster breakout 4x25GbE
swp3-14	nós de porta de cluster 40/100GbE
swp15-16	Portas de link entre switches (ISL) de 100 GbE

Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.

Atrasos na conexão com ligações ópticas

Se você estiver enfrentando atrasos na conexão superiores a cinco segundos, o Cumulus Linux 5.4 e versões posteriores incluem suporte para conexão rápida. Você pode configurar os links usando o `nv set` O comando é o seguinte:

```
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 seguintes ao `/etc/cumulus/switchd.conf` Arquivo para cada porta (swp<n>) que utiliza 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 o `switchd` 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` O comando é o seguinte:

- ° `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 Knowledge Base ["O switch SN2100 não consegue se conectar 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 placas de rede X1151A, placas de rede X1146A ou portas 100GbE integradas. Por exemplo:

- AFF A800 nas portas e0a e e0b
- AFF A320 nas portas e0g e e0h

Módulo QSA

Ao usar adaptadores QSFP+ (40GbE) para SFP+ (10GbE) ou adaptadores QSFP28 (100GbE) para SFP28 (25GbE) (QSA), insira-os em portas de switch 40GbE/100GbE não breakout (swp3-swp14). Não insira o módulo QSA em uma porta configurada para breakout.

Quando um módulo QSA é usado para conectar-se às portas de cluster 10GbE/25GbE em uma plataforma, a conexão pode não ser estabelecida.

Para resolver esse problema, faça o seguinte:

- Para 10GbE, defina manualmente a velocidade da conexão para 10000 e desative a negociação automática.
- Para conexões de 25GbE, defina manualmente a velocidade da conexão para 25000 e desative a negociação automática.

Configurar a velocidade da interface nas portas de breakout.

Dependendo do transceptor na porta do switch, pode ser necessário definir a velocidade na interface do switch para uma velocidade fixa. Se estiver usando portas breakout de 10GbE e 25GbE ou um módulo QSA, verifique se a negociação automática está desativada e configure 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 o status da interface e da porta para confirmar se as configurações foram 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
duplex	full	full
speed	10G	10G
fec	auto	auto
mtu	9216	9216
[breakout]		
state	up	up

Verifique o status da interface e da porta para confirmar se as configurações foram 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)						
.						
.						

Consulte o ["Hardware Universe"](#) e o artigo da Knowledge Base ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para mais informações.

O que vem a seguir?

Após analisar os requisitos de cabeamento e configuração, você pode ["Conecte os racks NS224 como armazenamento conectado por switch."](#) .

Conecte as prateleiras NS224 como armazenamento com interruptor.

Se você possui um sistema no qual os gabinetes de unidades NS224 precisam ser cabeados como armazenamento conectado por switch (e não como armazenamento conectado diretamente), utilize as informações fornecidas aqui.

- O cabo NS224 aciona as prateleiras através dos switches de armazenamento:

["Compartimentos de unidades NS224 conectados por switch de cabeamento"](#)

- Confirme o hardware compatível, como switches de armazenamento e cabos, para o modelo da sua plataforma. Consulte a ["Hardware Universe"](#) para obter detalhes.

O que vem a seguir?

Depois de instalar os cabos nas suas prateleiras, você pode ["configurar o switch"](#) .

Configurar o software

Fluxo de trabalho de instalação de software para switches NVIDIA SN2100

Para instalar e configurar o software de um switch NVIDIA SN2100, siga estes passos:

1

["Configure o interruptor"](#)

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 do Arquivo de Configuração de Referência \(RCF\)."](#)

Existem dois scripts RCF disponíveis para aplicações de Clustering e Armazenamento. O procedimento é o mesmo para todos.

6

["Instale o arquivo CSHM"](#)

Você pode instalar o arquivo de configuração aplicável para o monitoramento da integridade dos switches

Ethernet em clusters NVIDIA .

Configure o switch NVIDIA SN2100

Para configurar o switch SN2100, consulte a documentação da NVIDIA.

Passos

1. Analise o ["requisitos de configuração"](#) .
2. Siga as instruções em ["Inicialização do sistema NVIDIA ."](#) .

O que vem a seguir?

Depois de configurar o seu switch, você pode ["Instale o Cumulus Linux no modo Cumulus."](#) ou ["Instalar o Cumulus Linux no modo ONIE"](#) .

Instale o Cumulus Linux no modo Cumulus.

Siga este procedimento para instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver em modo Cumulus.



O sistema operacional Cumulus Linux (CL) pode ser instalado quando o switch está executando Cumulus Linux ou ONIE (consulte ["Instalar no modo ONIE"](#)).

Antes de começar

Certifique-se de ter o seguinte:

- Conhecimento intermediário de Linux.
- Familiaridade com edição básica de texto, permissões de arquivos UNIX e monitoramento de processos. Diversos editores de texto vêm pré-instalados, incluindo: `vi` e `nano` .
- Acesso a um shell Linux ou UNIX. Se você estiver usando o Windows, utilize um ambiente Linux como ferramenta de linha de comando para interagir com o Cumulus Linux.
- A taxa de transmissão (baud rate) exigida no switch de console serial para acesso ao console do switch NVIDIA SN2100 é de 115200, conforme segue:
 - 115200 baud
 - 8 bits de dados
 - 1 bit de parada
 - paridade: nenhuma
 - Controle de fluxo: nenhum

Sobre esta tarefa

Esteja ciente do 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 cumulus é **cumulus**. Na primeira vez que você fizer login no Cumulus Linux, você deverá alterar esta senha padrão. Certifique-se de atualizar todos os scripts de automação antes de instalar uma nova imagem. O Cumulus Linux oferece 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. Faça login no switch.

O primeiro acesso ao switch requer o nome de usuário/senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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. Atualização para o novo fuso horário:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

- c. Verifique seu 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. Configure 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 valor do 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 utiliza 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 o download. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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-o ao `sudo` grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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. Faça login no switch.

O primeiro acesso ao switch requer o nome de usuário/senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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 seu 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. Configure 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 valor do 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
```

Consulte o artigo da Knowledge Base ["A configuração do servidor NTP não está funcionando com switches NVIDIA SN2100."](#) para obter 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 utiliza 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 o download. Digite y quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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 cada nó possui 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-o ao `sudo` grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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 o usuário administrador acessar. `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 NVIDIA](#)" para mais informações.

Cumulus Linux 5.11.0

1. Faça login no switch.

Ao fazer login no switch pela primeira vez, é necessário inserir o nome de usuário e a senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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 seu 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. Configure 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 valor do 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
```

Consulte o artigo da Knowledge Base ["A configuração do servidor NTP não está funcionando com switches NVIDIA SN2100."](#) para obter 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 utiliza 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 o download. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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 possui 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 NVIDIA](#)" para mais informações.

O que vem a seguir?

Depois de instalar o Cumulus Linux no modo Cumulus, você "[Instale o script do Arquivo de Configuração de Referência \(RCF\)](#)".

Instale o Cumulus Linux no modo ONIE.

Siga este procedimento para instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver em modo ONIE.



O sistema operacional Cumulus Linux (CL) pode ser instalado quando o switch está executando ONIE ou Cumulus Linux (consulte "[Instalar no modo Cumulus](#)").

Sobre esta tarefa

Você pode instalar o Cumulus Linux usando o Open Network Install Environment (ONIE), que permite a descoberta automática de uma imagem de instalação de rede. Isso facilita o modelo de sistema para proteger switches com uma opção de sistema operacional, como o Cumulus Linux. A maneira mais fácil de instalar o Cumulus Linux com ONIE é através da descoberta HTTP local.



Se o seu host estiver habilitado para IPv6, certifique-se de que ele esteja executando um servidor web. Se o seu host estiver habilitado para IPv4, certifique-se de que ele esteja executando o DHCP além de um servidor web.

Este procedimento demonstra como atualizar o Cumulus Linux depois que o administrador inicializou o

sistema no ONIE.

Exemplo 2. Passos

Cumulus Linux 4.4.3

1. Faça o download do arquivo de instalação do Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo para: `onie-installer`.
2. Conecte seu computador à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interruptor.

O switch baixa o instalador de imagem ONIE e inicializa. Após a conclusão da instalação, a tela 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. Na tela do GNU GRUB, pressione a tecla **Esc** para interromper o processo normal de inicialização, selecione **ONIE** e pressione **Enter**.
6. Na tela seguinte, selecione **ONIE: Instalar SO**.
7. O processo de descoberta do instalador ONIE é executado em busca da instalação automática. Pressione **Enter** para interromper temporariamente o processo.
8. Quando o processo de descoberta for concluído:

```
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 sua rede, verifique se o endereço IP, a máscara de sub-rede e o gateway padrão estão atribuídos corretamente:

```
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 inseridas corretamente.

12. Instalar 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, faça login no switch.

```

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 do 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. Faça o download do arquivo de instalação do Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo para: `onie-installer`.
2. Conecte seu computador à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interruptor.

O switch baixa o instalador de imagem ONIE e inicializa. Após a conclusão da instalação, a tela 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. Na tela do GNU GRUB, pressione a tecla Esc para interromper o processo normal de inicialização, 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 SO**.

6. O processo de descoberta do instalador ONIE é executado em busca da instalação automática. Pressione **Enter** para interromper temporariamente o processo.
7. Quando o processo de descoberta for concluído:

```

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, faça login no switch.

```

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 do 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-o ao `sudo` grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```

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 o usuário administrador acessar. `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 NVIDIA](#)" para mais informações.

O que vem a seguir?

Após instalar o Cumulus Linux no modo ONIE, você pode "[Instale o script do Arquivo de Configuração de Referência \(RCF\)](#)."

Atualizar versões do Cumulus Linux

Siga o procedimento abaixo para atualizar sua versão do Cumulus Linux, conforme necessário.

Antes de começar

Certifique-se de ter o seguinte:

- Conhecimento intermediário de Linux.
- Familiaridade com edição básica de texto, permissões de arquivos UNIX e monitoramento de processos. Diversos editores de texto vêm pré-instalados, incluindo: `vi` e `nano`.
- Acesso a um shell Linux ou UNIX. Se você estiver usando o Windows, utilize um ambiente Linux como ferramenta de linha de comando para interagir com o Cumulus Linux.
- A taxa de transmissão (baud rate) exigida no switch de console serial para acesso ao console do switch NVIDIA SN2100 é de 115200, conforme segue:
 - 115200 baud
 - 8 bits de dados
 - 1 bit de parada
 - paridade: nenhuma
 - Controle de fluxo: nenhum

Sobre esta tarefa

Esteja ciente do seguinte:



Cada vez que o Cumulus Linux é atualizado, toda a estrutura do sistema de arquivos é apagada e reconstruída. Sua configuração atual será apagada. Você deve salvar e registrar a configuração do seu switch antes de atualizar o Cumulus Linux.



A senha padrão para a conta de usuário cumulus é **cumulus**. Na primeira vez que você fizer login no Cumulus Linux, você deverá alterar esta senha padrão. Você deve atualizar todos os scripts de automação antes de instalar uma nova imagem. O Cumulus Linux oferece opções de linha de comando para alterar a senha padrão automaticamente durante o processo de instalação.

Consulte "[Instalando uma nova imagem do Cumulus Linux](#)" para obter mais informações.

Exemplo 3. Passos

Cumulus Linux 4.4.x para Cumulus Linux 5.4.0

1. Conecte o switch do cluster à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 conectadas:

```
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. Baixe a imagem do Cumulux 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 senha:

```
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 do 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. Alterar 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/syncd/syncd.conf
.
.
```

12. Saia da sessão e entre novamente no switch para ver o nome atualizado do switch 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 5.10.0-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-o ao sudo grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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 o usuário administrador acessar. `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 o ["Contas de usuário NVIDIA"](#) para mais informações.

Cumulus Linux 5.x para Cumulus Linux 5.4.0

1. Conecte o switch do cluster à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 conectadas:


```

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. Baixe a imagem do Cumulux 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 senha:

```
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 do 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. Alterar 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/syncd/syncd.conf
.
.
```

12. Saia da sessão e entre novamente no switch para ver o nome atualizado do switch 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 5.10.0-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-o ao sudo grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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 o usuário administrador acessar. `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 NVIDIA](#)" para mais informações.

Cumulus Linux 5.4.0 para Cumulus Linux 5.11.0

1. Conecte o switch do cluster à rede de gerenciamento.
2. Utilize o comando ping para verificar a conectividade com o servidor que hospeda o Cumulus Linux e o RCF.
3. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 conectadas:

```

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. Baixe a imagem do Cumulux 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 senha:


```
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 do 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. Alterar 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/syncd/syncd.conf
.
.
```

12. Saia da sessão e entre novamente no switch para ver o nome atualizado do switch 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 vem a seguir?

Após atualizar sua versão do Cumulus Linux, você poderá ["Instalar ou atualizar o script RCF"](#) .

Instale ou atualize o script do Arquivo de Configuração de Referência (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 os seguintes itens estejam disponíveis no switch:

- Cumulus Linux está instalado. Consulte a ["Hardware Universe"](#) para versões suportadas.

- Endereço IP, máscara de sub-rede e gateway padrão definidos via DHCP ou configurados manualmente.



Você deve especificar um usuário no RCF (além do usuário administrador) para ser usado especificamente para a coleta de logs.

Configurações do cliente

As seguintes categorias de configuração de referência estão disponíveis:

Conjunto	Em portas configuradas para breakout 4x10GbE, uma porta é configurada para breakout 4x25GbE e as demais portas são configuradas para 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas para nós que utilizam portas compartilhadas de cluster/HA. Consulte a tabela de plataformas no artigo da Knowledge Base "Quais plataformas AFF, ASA e FAS usam portas Ethernet de cluster e HA compartilhadas?" . Todas as portas também podem ser usadas como portas dedicadas de cluster.
Armazenar	Todas as portas configuradas para conexões de armazenamento NVMe de 100 GbE.

Versões atuais do script RCF

Existem dois scripts RCF disponíveis para aplicações de Cluster e Armazenamento. Baixe os RCFs de ["Download do software NVIDIA SN2100"](#) página. O procedimento é o mesmo para todos.

- Cluster: **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**
- Armazenamento: **MSN2100-RCF-v1.x-Armazenamento**

Sobre os exemplos

O procedimento de exemplo a seguir mostra como baixar e aplicar o script RCF para switches de cluster.

O comando de exemplo utiliza o endereço IP de gerenciamento do 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. Conecte o switch do 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. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 desativar a reversão automática nesta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desativar a reversão automática para esta etapa, pois ela já está desativada.

1. Exibir as interfaces disponíveis no switch 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` Se o método utilizado for o do exemplo, você pode usar o 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 executa as etapas listadas no exemplo acima.



Na etapa 3 **Atualizando o arquivo MOTD** acima, o comando `cat /etc/motd` é executado. Isso permite verificar o nome do arquivo RCF, a versão do RCF, as portas a serem usadas e outras informações importantes no banner do RCF.



Para quaisquer problemas com o script Python do RCF que não possam ser corrigidos, entre em contato com "[Suporte NetApp](#)" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Análise as considerações sobre cabeamento e configuração.](#)" 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 transceptor 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 cada nó possui 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 do cluster.

- a. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

- b. Verifique o estado de saúde do switch no cluster (o switch sw2 pode não ser exibido, pois as LIFs

não estão configuradas em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol	Local Port	Discovered 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 Model	Type	Address

sw1 MSN2100-CB2RC	cluster-network	10.233.205.90
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 MSN2100-CB2RC	cluster-network	10.233.205.91
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 íntegro:

```
cluster show
```

10. Repita os passos de 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. Conecte o switch do 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. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 desativar a reversão automática nesta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desativar a reversão automática para esta etapa, pois ela já está desativada.

1. Exibir as interfaces disponíveis no switch 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` Se o método utilizado for o do exemplo, você pode usar o 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 executa 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 do RCF, as portas a serem usadas e outras informações importantes no banner do 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 com o script Python do RCF que não possam ser corrigidos, entre em contato com "[Suporte NetApp](#)" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Análise as considerações sobre cabeamento e configuração.](#)" 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: fd20:8ble: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 transceptor 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 cada nó possui 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 do cluster.

a. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

b. Verifique o estado de saúde do switch no cluster (o switch sw2 pode não ser exibido, pois as LIFs

não estão configuradas em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol	Local Port	Discovered 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 Model	Type	Address

sw1 MSN2100-CB2RC	cluster-network	10.233.205.90
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 MSN2100-CB2RC	cluster-network	10.233.205.91
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 íntegro:

```
cluster show
```

10. Repita os passos de 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. Conecte o switch do 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. Exibir as portas do cluster em cada nó que estão conectadas aos switches do cluster:

```
network device-discovery show
```

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

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

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

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 desativar a reversão automática nesta etapa.
- Se você acabou de atualizar sua versão do Cumulus Linux, não precisa desativar a reversão automática para esta etapa, pois ela já está desativada.

1. Exibir as interfaces disponíveis no switch 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` Se o método utilizado for o do exemplo, você pode usar o 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 executa 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 do RCF, as portas a serem usadas e outras informações importantes no banner do 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 com o script Python do RCF que não possam ser corrigidos, entre em contato com "[Suporte NetApp](#)" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Análise as considerações sobre cabeamento e configuração.](#)" 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: fd20:8ble: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 transceptor 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 cada nó possui 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 do cluster.

a. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

b. Verifique o estado de saúde do switch no cluster (o switch sw2 pode não ser exibido, pois as LIFs

não estão configuradas em e0d).

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol	Local Port	Discovered 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 Model	Type	Address

sw1 MSN2100-CB2RC	cluster-network	10.233.205.90
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 MSN2100-CB2RC	cluster-network	10.233.205.91
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 íntegro:

```
cluster show
```

10. Repita os passos de 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 vem a seguir?

Após instalar o RCF, você pode ["Instale o arquivo CSHM"](#).

Instale o arquivo de configuração do Monitor de Saúde do Switch Ethernet.

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

Estas instruções aplicam-se caso as chaves NVIDIA X190006-PE e X190006-PI não sejam detetadas corretamente, o que pode ser confirmado executando o seguinte comando: `system switch ethernet show` e verificando se **OUTRO** 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 versões 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 saúde e a coleta de registros possam funcionar mesmo sem essas etapas, segui-las garante que tudo opere 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 ONTAP esteja ativo e em funcionamento.
- 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 shell do nó:

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

- b. Alteração para privilégios avançados:

```
priv set advanced
```

- c. Liste os arquivos de configuração em `/etc/cshm_nod/nod_sign` diretório. Se o diretório existir e contiver arquivos de configuração, ele listará os nomes dos arquivos.

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

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

Caso não tenha certeza, remova todos os arquivos de configuração dos modelos compatíveis listados acima e, em seguida, baixe e instale os arquivos 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. Baixe o arquivo zip de configuração do monitor de integridade do switch Ethernet, de acordo com a versão do ONTAP correspondente. Este arquivo está disponível em ["Switches Ethernet NVIDIA"](#) página.
 - a. Na página de download do software NVIDIA SN2100, selecione **Arquivo CSHM da NVIDIA**.
 - b. Na página de Atenção/Leitura Obrigatória, selecione a caixa de seleção para concordar.
 - c. Na página do Contrato de Licença do Usuário Final, selecione a caixa de seleção para concordar e clique em **Aceitar e Continuar**.
 - d. Na página de download do arquivo CSHM da Nvidia, selecione o arquivo de configuração aplicável. Os seguintes arquivos estão disponíveis:

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 a 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. [[passo 2]]Faça o upload do arquivo zip correspondente para o seu servidor web interno.
2. Acesse as configurações do modo avançado a partir de um dos sistemas ONTAP no cluster.

```
set -privilege advanced
```

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

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

4. Verifique se a saída do comando termina com o seguinte texto para a 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 a 9.14.1

O SHM instalou o arquivo de configuração.

ONTAP 9.10.1

O pacote CSHM foi baixado e processado com sucesso.

Caso ocorra algum erro, entre em contato com o suporte da NetApp .

1. [[passo 6]]Aguarde até o dobro do intervalo de sondagem do monitor de integridade do switch Ethernet, determinado executando `system switch ethernet polling-interval show` , antes de concluir a próxima etapa.
2. Execute o comando `system switch ethernet configure-health-monitor show` No sistema ONTAP , certifique-se de que os switches do cluster sejam descobertos com o campo monitorado definido como **Verdadeiro** e o campo do número de série não mostrando **Desconhecido**.

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



Se o seu modelo ainda estiver exibindo **OUTRO** após a aplicação do arquivo de configuração, entre em contato com o suporte da NetApp .

Veja o "[switch de sistema ethernet configurar-monitor-de-saúde](#)" Para mais detalhes, entre em contato.

O que vem a seguir?

Após instalar o arquivo CSHM, você pode "[configurar 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 o Cumulus Linux 5.11 e versões posteriores, você usa o `nv action reset system factory-default` comando.

Sobre esta tarefa

- Você precisa estar conectado ao switch usando o console serial.
- Você precisa ter a senha de root para ter acesso sudo aos comandos.



Para 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. A partir do console do Cumulus, baixe e coloque na fila a instalação do software do switch com o comando `onie-install -a -i` seguido do caminho do arquivo do software de comutação, 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 reinicia e permanece no estado em que foi instalado. `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
```

Consulte a documentação da ["Redefinição de fábrica"](#) NVIDIA para obter mais detalhes.

O que vem a seguir

Depois de reiniciar os interruptores, você pode ["reconfigurar"](#) eles conforme necessário.

Migre os switches

Migrar switches de cluster CN1610 para switches de cluster NVIDIA SN2100

Você pode migrar switches de cluster NetApp CN1610 de um cluster ONTAP para switches de cluster NVIDIA SN2100. Este é um procedimento não disruptivo.

Requisitos de revisão

Você deve estar ciente de certas informações de configuração, conexões de porta e requisitos de cabeamento ao substituir os switches de cluster NetApp CN1610 por switches de cluster NVIDIA SN2100. Consulte ["Visão geral da instalação e configuração dos switches NVIDIA SN2100"](#).

Interruptores 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 configurado corretamente e funcionando.
- Todas as portas do cluster estão no estado **ativo** para garantir operações sem interrupções.
- Os switches de cluster NVIDIA SN2100 estão configurados e operando com a versão correta do Cumulus Linux instalada e com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede do cluster existente apresenta as seguintes características:
 - Um cluster NetApp redundante e totalmente funcional usando switches CN1610.
 - Conectividade de gerenciamento e acesso ao console tanto para os switches CN1610 quanto para os novos switches.
 - Todas as LIFs do cluster estão ativas, com as LIFs do cluster em suas portas de origem.
 - As portas ISL foram habilitadas e conectadas por cabos entre os switches CN1610 e entre os novos switches.
- Algumas portas dos switches NVIDIA SN2100 estão configuradas para operar em 40GbE ou 100GbE.
- Você planejou, migrou e documentou a conectividade de 40GbE e 100GbE dos nós para os switches de cluster NVIDIA SN2100.

Migre os switches

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os switches de cluster CN1610 existentes são *c1* e *c2*.
- Os novos switches de cluster NVIDIA SN2100 são *sw1* e *sw2*.
- Os nós são *node1* e *node2*.

- Os LIFs do cluster são *node1_clus1* e *node1_clus2* no nó 1, e *node2_clus1* e *node2_clus2* no nó 2, respectivamente.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *e3a* e *e3b*.
- As portas de breakout têm o seguinte formato: `swp[porta]s[porta de breakout 0-3]`. Por exemplo, quatro portas breakout em `swp1` são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O interruptor `c2` é substituído primeiro pelo interruptor `sw2`.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Em seguida, o cabeamento entre os nós e o `c2` é desconectado do `c2` e reconectado ao `sw2`.
- O interruptor `c1` é substituído pelo interruptor `sw1`.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - Em seguida, o cabeamento entre os nós e `c1` é desconectado de `c1` e reconectado a `sw1`.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Etapa 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (***>**) é exibida.

3. Desativar a reversão automática nas LIFs do cluster:

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

Etapa 2: Configurar portas e cabos

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

Cada porta deve aparecer para cima. `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

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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 respectivos nós de origem:

```
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
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 do cluster em cada nó são conectadas aos switches de cluster existentes da seguinte maneira (da perspectiva dos nós), utilizando 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 switches do cluster estão conectados da seguinte forma (do ponto de vista 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	0/1	124	H	AFF-A400
node2 e3a	0/2	124	H	AFF-A400
c2 0/13	0/13	179	S I s	CN1610
c2 0/14	0/14	175	S I s	CN1610
c2 0/15	0/15	179	S I s	CN1610
c2 0/16	0/16	175	S I s	CN1610

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	0/1	124	H	AFF-A400
node2 e3b	0/2	124	H	AFF-A400
c1 0/13	0/13	175	S I s	CN1610
c1 0/14	0/14	175	S I s	CN1610
c1 0/15	0/15	175	S I s	CN1610
c1 0/16	0/16	175	S I s	CN1610

4. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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. **[[passo 5]]**No switch c2, desligue as portas conectadas às portas do cluster dos nós para realizar o 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 a cablagem apropriada compatível com o 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
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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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, desligue as portas conectadas às portas do cluster dos nós para realizar o 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 a cablagem apropriada compatível com o NVIDIA SN2100.
8. Verifique a configuração final do cluster:

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

Cada porta deve exibir 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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 possuem uma conexão com cada switch:

```
net show lldp
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 reversão automática nos LIFs do cluster:

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

2. No switch sw2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. [[passo 3]]Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

3. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migrar de um switch de cluster Cisco para um switch de cluster NVIDIA SN2100

Você pode migrar switches de cluster Cisco de um cluster ONTAP para switches de cluster NVIDIA SN2100. Este é um procedimento não disruptivo.

Requisitos de revisão

Você deve estar ciente de certas informações de configuração, conexões de porta e requisitos de cabeamento ao substituir alguns switches de cluster Cisco mais antigos por switches de cluster NVIDIA SN2100. Consulte ["Visão geral da instalação e configuração dos switches NVIDIA SN2100"](#).

Interruptores suportados

Os seguintes switches de cluster da 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

Assegure-se de que:

- O cluster existente está configurado corretamente e funcionando.
- Todas as portas do cluster estão no estado **ativo** para garantir operações sem interrupções.
- Os switches de cluster NVIDIA SN2100 estão configurados e operando sob a versão adequada do Cumulus Linux instalada com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede do cluster existente apresenta as seguintes características:
 - Um cluster NetApp redundante e totalmente funcional, utilizando switches Cisco mais antigos.
 - Conectividade de gerenciamento e acesso ao console tanto para os switches Cisco mais antigos quanto para os novos.
 - Todas as LIFs do cluster estão ativas e conectadas às suas portas de origem.
 - As portas ISL foram habilitadas e cabeadas entre os switches Cisco mais antigos e entre os novos switches.
- Algumas portas dos switches NVIDIA SN2100 estão configuradas para operar em 40 GbE ou 100 GbE.
- Você planejou, migrou e documentou a conectividade de 40 GbE e 100 GbE dos nós para os switches de cluster NVIDIA SN2100.



Se você estiver alterando a velocidade das portas de cluster e0a e e1a em sistemas AFF A800 ou AFF C800, poderá observar o recebimento de pacotes malformados após a conversão de velocidade. Consulte ["Erro 1570339"](#) e o artigo da Knowledge Base ["Erros de CRC em portas T6 após conversão de 40GbE para 100GbE"](#) para obter orientações.

Migre os switches

Sobre os exemplos

Neste procedimento, os switches de cluster Cisco Nexus 3232C são usados como exemplos de comandos e saídas.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os switches de cluster Cisco Nexus 3232C existentes são *c1* e *c2*.
- Os novos switches de cluster NVIDIA SN2100 são *sw1* e *sw2*.
- Os nós são *node1* e *node2*.
- Os LIFs do cluster são *node1_clus1* e *node1_clus2* no nó 1, e *node2_clus1* e *node2_clus2* no nó 2, respectivamente.
- O `cluster1::*>` prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *e3a* e *e3b*.
- As portas de breakout têm o seguinte formato: `swp[porta]s[porta de breakout 0-3]`. Por exemplo, quatro portas breakout em `swp1` são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre esta tarefa

Este procedimento abrange o seguinte cenário:

- O interruptor *c2* é substituído primeiro pelo interruptor *sw2*.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - A fiação entre os nós e o *c2* é então desconectada do *c2* e reconectada ao *sw2*.
- O interruptor *c1* é substituído pelo interruptor *sw1*.
 - Desative as portas dos nós do cluster. Todas as portas devem ser desligadas simultaneamente para evitar instabilidade no cluster.
 - A fiação entre os nós e *c1* é então desconectada de *c1* e reconectada a *sw1*.

Etapa 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (***>**) é exibida.

3. Desativar a reversão automática nas LIFs do cluster:

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

Etapa 2: Configurar portas e cabos

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

Cada porta deve aparecer para cima. 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					
Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper

e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2					
Ignore					
Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper

e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Exibir informações sobre as interfaces lógicas e seus respectivos nós de origem:

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

Cada LIF deve exibir up/up para Status Admin/Oper e é verdade 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 do cluster em cada nó estão conectadas aos switches de cluster existentes da seguinte forma (da perspectiva 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 switches do cluster estão conectados da seguinte forma (do ponto de vista 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
c2 Eth1/31	Eth1/31	179	S I s	N3K-C3232C
c2 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
c1 Eth1/31	Eth1/31	175	S I s	N3K-C3232C
c1 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

4. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 5]] No switch c2, desligue as portas conectadas às portas do cluster dos nós para realizar o 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 a cablagem apropriada compatível com o 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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, desligue as portas conectadas às portas do cluster dos nós para realizar o 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 a cablagem apropriada compatível com o NVIDIA SN2100.
8. Verifique a configuração final do cluster:

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

Cada porta deve exibir 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva dos nós:

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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 possuem uma conexão com cada switch:

```
net show lldp
```


Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 reversão automática nos LIFs do cluster:

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

2. No switch sw2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. [[passo 3]]Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

3. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migre para um cluster comutado de dois nós com switches de cluster NVIDIA SN2100.

Se você já possui um ambiente de cluster sem switches com dois nós, pode migrar para um ambiente de cluster com switches com dois nós usando switches NVIDIA SN2100 para permitir a escalabilidade além de dois nós no cluster.

O procedimento a ser utilizado depende de você ter 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 utilizam portas ópticas ou Twinax, mas não é suportado neste switch se os nós estiverem utilizando portas RJ45 10GBASE-T integradas para as portas de rede do cluster.

Requisitos de revisão

Configuração sem switch de dois nós

Assegure-se de que:

- A configuração sem switch de dois nós está configurada corretamente e funcionando.
- Os nós estão executando o ONTAP 9.10.1P3 ou posterior.
- Todas as portas do cluster estão no estado **ativo**.
- Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e em suas portas de origem.

Configuração do switch de cluster NVIDIA SN2100

Assegure-se de que:

- Ambos os switches possuem conectividade de rede de gerenciamento.
- É possível acessar os switches do cluster através do console.
- As conexões entre nós e entre switches do NVIDIA SN2100 utilizam cabos Twinax ou de fibra óptica.



Consulte ["Análise as considerações sobre cabeamento e configuração."](#) para obter ressalvas e mais detalhes. O ["Hardware Universe - Switches"](#) também contém mais informações sobre cabeamento.

- Os cabos Inter-Switch Link (ISL) estão conectados às portas swp15 e swp16 em ambos os switches NVIDIA SN2100.
- A personalização inicial dos dois switches SN2100 foi 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 do 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 suas plataformas.

Migre os switches

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- Os nomes dos interruptores 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, respectivamente.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *e3a* e *e3b*.
- As portas de breakout têm o seguinte formato: `swp[porta]s[porta de breakout 0-3]`. Por exemplo, quatro portas breakout em `swp1` são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Etapas 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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`

O prompt avançado(**>*) aparece.

Etapas 2: Configurar portas e cabos

Cumulus Linux 4.4.x

1. Desative todas as portas voltadas para os nós (exceto as portas ISL) nos dois novos switches do cluster, sw1 e sw2.

Você 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 ativas nas portas swp15 e swp16:

```
net show interface
```

Os comandos a seguir mostram que as portas ISL estão ativas 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 os nós (exceto as portas ISL) nos dois novos switches do cluster, sw1 e sw2.

Você 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 ativas nas portas swp15 e swp16:

```
nv show interface
```

Os exemplos a seguir mostram que as portas ISL estão ativas 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	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-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	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

1. [[passo 3]] Verifique se todas as portas do cluster estão ativas:

```
network port show
```

Cada porta deve exibir up para Link e saudável para Health Status .

Mostrar exemplo

```
cluster1::*> network port show
```

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 do cluster estão ativas e operacionais:

```
network interface show
```

Cada LIF de cluster deve exibir verdadeiro para Is Home e tenha 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 nas 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. Desconecte o cabo da porta do cluster e3a no nó 3 e, em seguida, conecte e3a à porta 1 no switch do cluster sw1, usando o cabeamento apropriado suportado pelos switches SN2100.

O "[Hardware Universe - Switches](#)" Contém mais informações sobre cabeamento.

5. Desconecte o cabo da porta do cluster e3a no nó 4 e, em seguida, conecte e3a à porta 2 no switch do

cluster sw1, usando o cabeamento apropriado suportado pelos switches SN2100.

Cumulus Linux 4.4.x

1. [[passo 8]] 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. [[passo 8]] 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. [[passo 9]] 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	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

1. [[passo 10]] 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 ativas no nó 1 e no nó 2:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 estado 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. Desconecte o cabo da porta do cluster e3b no nó 3 e, em seguida, conecte e3b à porta 1 no switch do cluster sw2, usando o cabeamento apropriado suportado pelos switches SN2100.
4. Desconecte o cabo da porta do cluster e3b no nó 4 e, em seguida, conecte e3b à porta 2 no switch do 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 seguintes comandos 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. [[passo 15]] 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 cada um dos nós possui uma conexão com cada switch:

```
net show lldp
```

O exemplo a seguir mostra os resultados apropriados para as chaves 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 seguintes comandos 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. [[passo 15]] 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	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

3. Em ambos os switches sw1 e sw2, verifique se cada um dos nós possui uma conexão com cada switch:

```
nv show interface --view=lldp
```

Os exemplos a seguir mostram os resultados apropriados para as chaves 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. Exibir 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 ativas no nó 1 e no nó 2:

```
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 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
```

Vserver	Logical Interface	Auto-revert
-----	-----	-----
Cluster		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

2. No switch sw2, desligue e reinicie todas as portas do cluster para acionar uma reversão automática de todas as LIFs do cluster que não estejam em suas portas de origem.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. [[passo 3]]Verifique se as LIFs do cluster retornaram às suas portas originais (isso pode levar um minuto):

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

Se alguma das LIFs do cluster não tiver retornado à sua porta original, reverta-as manualmente. Você deve se conectar a cada console de gerenciamento de nó LIF ou SP/ BMC do nó local que possui o LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Verifique se todas as interfaces exibem `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 todas as LIFs estão ativas no nó 1 e no nó 2 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 configurações estão desativadas:

```
network options switchless-cluster show
```

O resultado incorreto 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 nós membros do cluster:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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. [[passo 8]]Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Substitua os interruptores

Substitua um switch de cluster NVIDIA SN2100

Siga este procedimento para substituir um switch NVIDIA SN2100 defeituoso em uma rede de cluster. Este é um procedimento não disruptivo (NDU).

Requisitos de revisão

Infraestrutura de cluster e rede existente

Assegure-se de que:

- O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
- Todas as portas do cluster estão ativas.
- Todas as interfaces lógicas do cluster (LIFs) estão ativas e em suas portas de origem.
- O ONTAP `cluster ping-cluster -node node1` O comando indica que a conectividade básica e a comunicação com dispositivos maiores que PMTU estão funcionando corretamente em todos os caminhos.

Interruptor de substituição NVIDIA SN2100

Assegure-se de que:

- A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
- O acesso ao console do interruptor de substituição já está instalado.
- As conexões de nó são as portas swp1 a swp14.
- Todas as portas de Interconexão de Switches (ISL) estão desativadas nas portas swp15 e swp16.
- O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional Cumulus são carregados no switch.
- A personalização inicial do interruptor 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 migrar um LIF de cluster a partir do nó onde o LIF de cluster está hospedado.

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster em cada nó são denominadas *e3a* e *e3b*.
- Os nomes LIF do cluster são *node1_clus1* e *node1_clus2* para o nó 1, e *node2_clus1* e *node2_clus2* para o nó 2.
- O aviso para alterações em todos os nós do cluster é `cluster1::*>`
- As portas de breakout têm o seguinte formato: `swp[porta]s[porta de breakout 0-3]`. Por exemplo, quatro portas breakout em `swp1` são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Sobre a topologia da rede do cluster

Este procedimento baseia-se na seguinte topologia de rede em cluster:

Mostrar exemplo de topologia

cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

Node: node2

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

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	-	

+

```
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

Etapas 1: Prepare-se para a substituição

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Instale o RCF e a imagem apropriados no switch, nsw2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e Cumulus para o novo switch.

- a. Você pode baixar o software Cumulus aplicável aos seus switches de cluster no site de suporte da NVIDIA. Siga os passos na página de Download para baixar o Cumulus Linux para a versão do software ONTAP que você está instalando.
- b. O RCF apropriado está disponível em "[Switches de cluster e armazenamento NVIDIA](#)" página. Siga os passos na página de Download para baixar o RCF correto para a versão do software ONTAP que você está instalando.

Etapas 2: Configurar portas e cabos

Cumulus Linux 4.4.3

1. No novo switch nsw2, faça login como administrador e desative todas as portas que serão conectadas às interfaces do cluster de nós (portas swp1 a swp14).

As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em 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 nas 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 todas as LIFs do cluster têm a reversão automática desativada:

```
net interface show -vserver Cluster -fields auto-revert
```

4. Desligue as portas ISL swp15 e swp16 no switch 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, em seguida, conecte-os às mesmas portas do switch SN2100 nsw2.
6. Ative as portas ISL swp15 e swp16 entre os switches sw1 e nsw2.

Os seguintes comandos habilitam as portas ISL swp15 e swp16 no switch 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 ativas no switch 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 ativas no switch 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 essa porta e3b Está ativo em todos os nós:

```
network port show -ipSpace Cluster
```

O resultado deverá 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva 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 possuem uma conexão com cada switch:

```
net show lldp
```

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 reversão automática nos LIFs do cluster:

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

12. No switch nsw2, ative as portas conectadas 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 o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	true	true
node2	true	true

14. Verifique se todas as portas físicas do cluster 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 desative todas as portas que serão conectadas às interfaces do cluster de nós (portas swp1 a swp14).

As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em cada nó.

```
cumulus@nsw2:~$ nv set interface swp15-16 link state down
cumulus@nsw2:~$ nv config apply
```

2. Desativar a reversão automática nas 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 todas as LIFs do cluster têm a reversão automática desativada:

```
network interface show -vserver Cluster -fields auto-revert
```

4. Desligue as portas ISL swp15 e swp16 no switch 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, em seguida, conecte-os às mesmas portas do switch SN2100 nsw2.
6. Ative as portas ISL swp15 e swp16 entre os switches sw1 e nsw2.

Os seguintes comandos habilitam as portas ISL swp15 e swp16 no switch 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 ativas no switch 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 ativas no switch 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 essa porta e3b Está ativo em todos os nós:

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

O resultado deverá 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 estão conectadas aos switches do cluster da seguinte maneira, da perspectiva 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 possuem uma conexão com cada switch:

```
nv show interface lldp
```

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 reversão automática nos LIFs do cluster:

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

12. No switch nsw2, ative as portas conectadas 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 o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	true	true
node2	true	true

14. Verifique se todas as portas físicas do cluster 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 íntegra.

```
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 íntegra.

```
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. [[passo 2]] Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

2. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar 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 uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

Requisitos de revisão

Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

Antes de começar

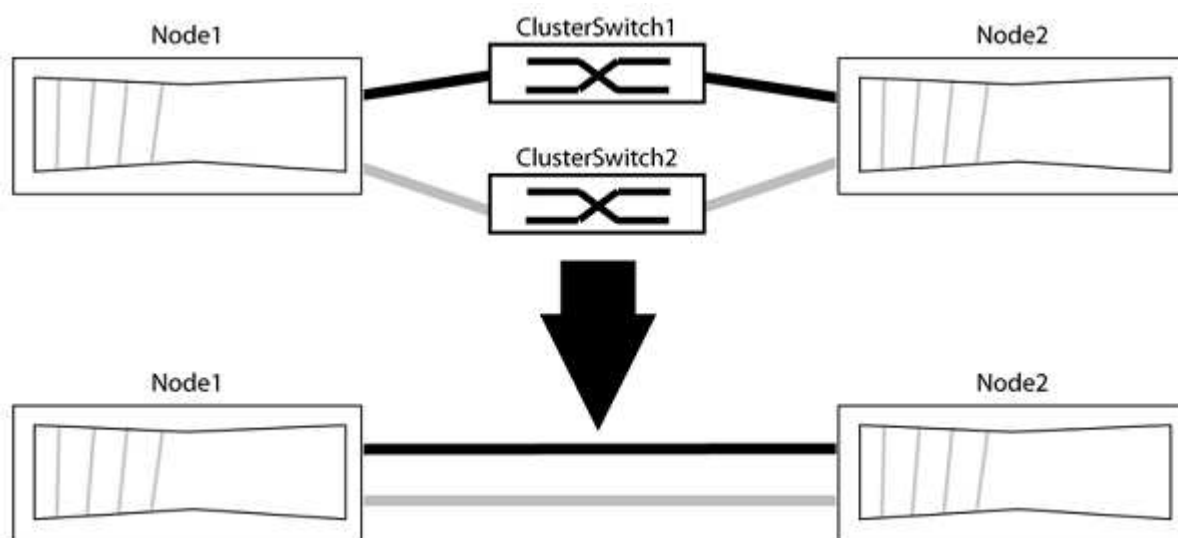
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migre 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 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 elas variam de acordo com o sistema.

Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

onde `h` é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

Mostrar exemplo

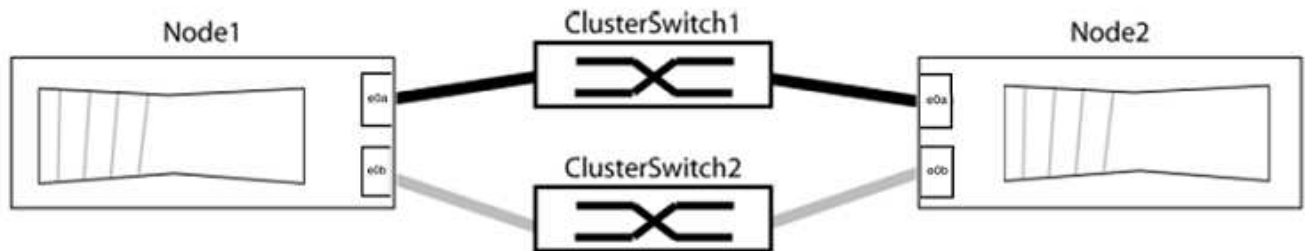
```
cluster::*> system node autosupport invoke -node * -type all
-mmessage MAINT=2h
```

Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Estado de Saúde".

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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está `true` para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

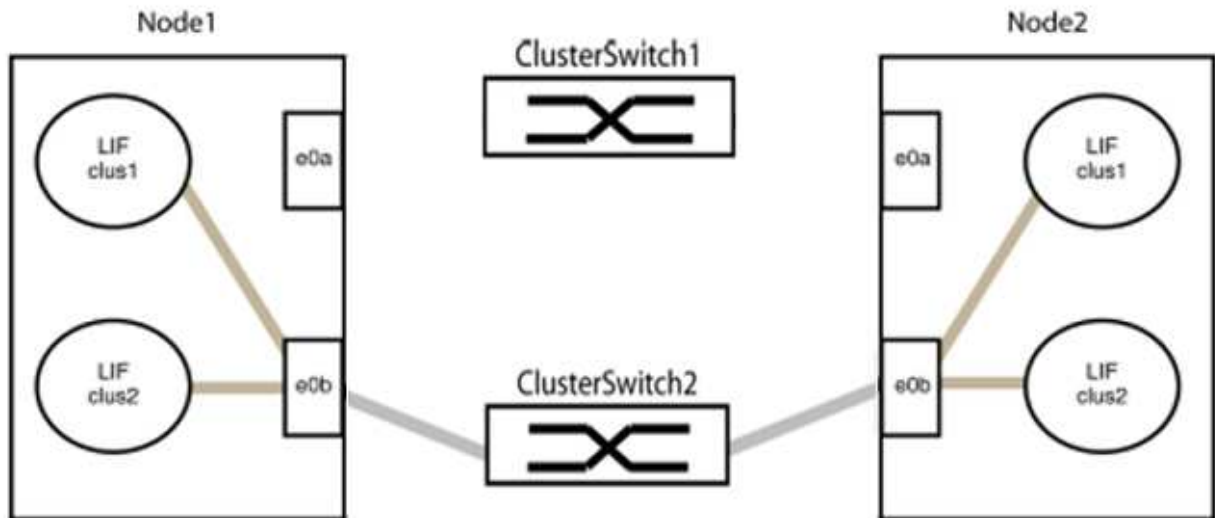
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

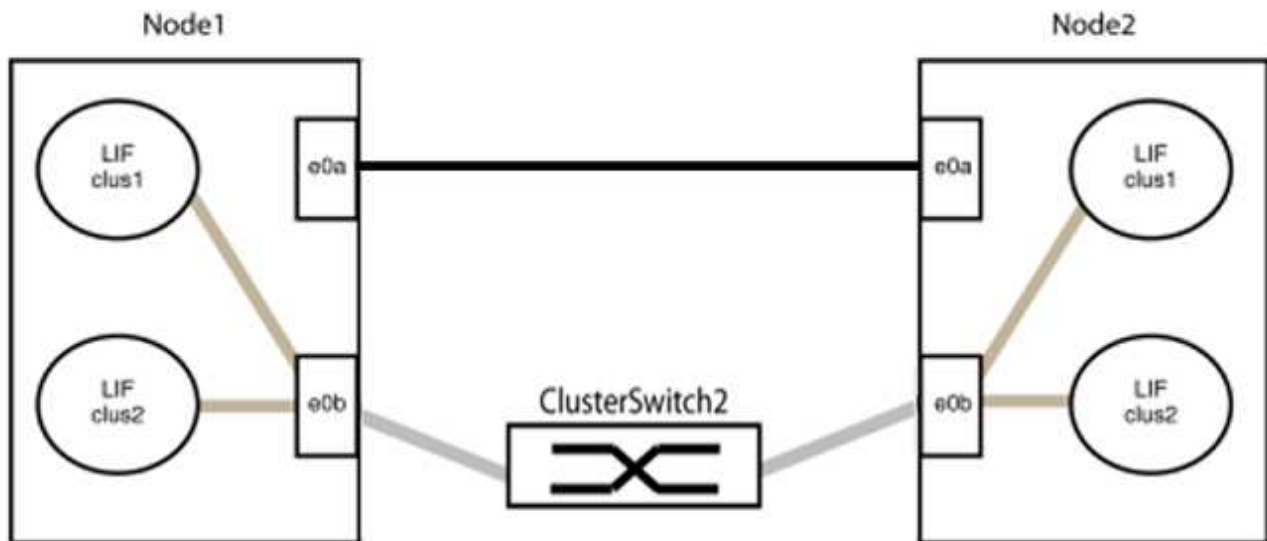
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

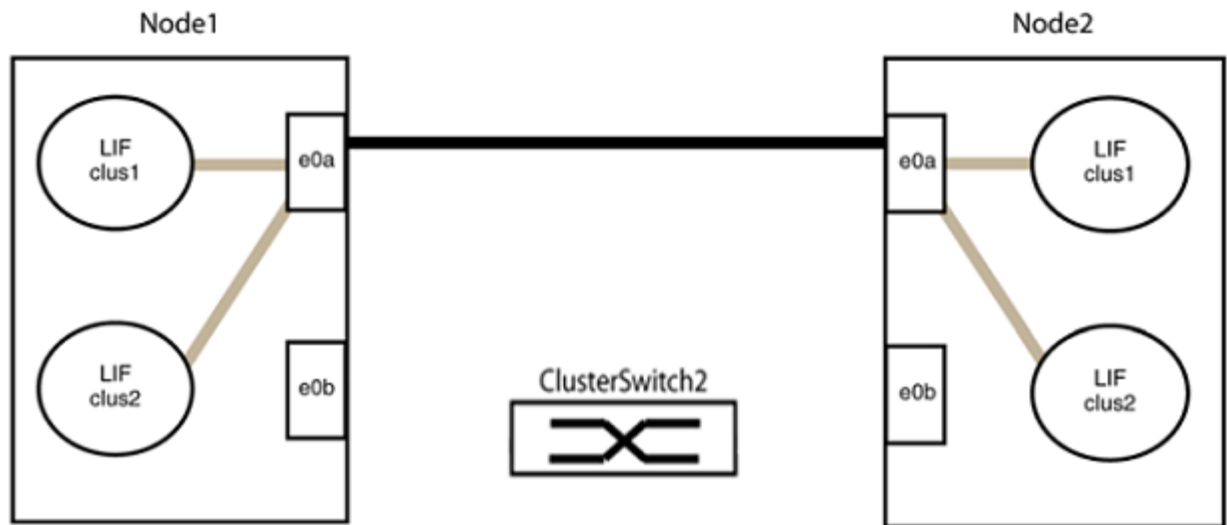
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna “Is Home” estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. **[[passo 6]]** Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Interruptores de armazenamento

Cisco Nexus 9336C-FX2 ou 9336C-FX2-T

Começar

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.

Requisitos de configuração

Para a configuração, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches.

Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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 o ["Hardware Universe"](#) para obter as informações mais recentes.

Para obter mais informações sobre a configuração inicial do seu switch, consulte o seguinte: ["Guia de Instalação e Atualização do Cisco Nexus 9336C-FX2"](#).

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

Componentes e números de peça para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para instalação e manutenção dos switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T, certifique-se de consultar a lista de componentes e números de peça.

A tabela a seguir lista o número da peça e a descrição dos switches de armazenamento 9336C-FX2 e 9336C-FX2-T, ventiladores e fontes de alimentação:

Número da peça	Descrição
X190200-CS-PE	Chave seletora de cluster, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Cluster Switch, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Chave seletora de cluster, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G

Número da peça	Descrição
X190212-CS-PI	Chave seletora de cluster, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	SW, Licença Cisco 9336CFX2 POD de 24 portas
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	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de exaustão lateral
X-NXA-PAC-1100W-PI2	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de entrada pelo lado da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65 CFM, fluxo de ar de exaustão do lado esquerdo
X-NXA-FAN-65CFM-PI	N9K-9336C 65 CFM, fluxo de ar de admissão pelo lado esquerdo

Licenças Cisco Smart somente para portas 9336C-FX2-T

Para ativar mais de 12 portas no seu switch de armazenamento Cisco Nexus 9336C-FX-T, você precisa adquirir uma licença Cisco Smart. As licenças Cisco Smart são gerenciadas por meio de contas Cisco Smart.

1. Crie uma nova conta Smart, se necessário. Consulte ["Crie uma nova conta Smart"](#) para obter detalhes.
2. Solicite acesso a uma conta Smart existente. Consulte ["Solicitar acesso a uma conta Smart existente"](#) para obter detalhes.



Após adquirir sua licença Smart, instale o RCF apropriado para habilitar e configurar todas as 36 portas disponíveis para uso.

O que vem a seguir

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Para a instalação 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 9336C-FX2 e o cluster ONTAP.

Documentação do Switch

Para configurar os switches Cisco Nexus 9336C-FX2, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 9000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 9000</i>	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 9000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 9000 Series NX-OS</i>	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 9000</i>	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 9000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 9000</i>	Descreve as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
<i>Notas de versão do NX-OS para a série Cisco Nexus 9000</i> (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.
Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 9000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .

Nome	Descrição
"ONTAP 9"	Fornece informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornece informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco 9336-FX2 em um NetApp cabinet, consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"Instale um switch Cisco 9336-FX2 em um gabinete NetApp."	Este manual descreve como instalar um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp de quatro postes.

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale os switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

3

"Instale o switch 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

"Analise as considerações sobre cabeamento e configuração."

Antes de configurar seus 9336C-FX2 e 9336C-FX2-T switches, revise as considerações de cabeamento e configuração.

Preencha a planilha de cabeamento do Cisco Nexus 9336C-FX2 ou 9336C-FX2-T.

Se você deseja documentar as plataformas suportadas, baixe o PDF desta página e preencha a planilha de cabeamento.

A planilha de cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

- [Folha de exercícios de cabeamento de amostra 9336C-FX2](#)
- [Folha de trabalho de cabeamento em branco 9336C-FX2](#)
- [Folha de exemplo de cabeamento 9336C-FX2-T \(12 portas\)](#)
- [Folha de trabalho de cabeamento em branco 9336C-FX2-T \(12 portas\)](#)

Folha de exercícios de cabeamento de amostra 9336C-FX2

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 1 com 4 conexões 100GbE	1	Nó 1 com 4 conexões 100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
2	Nó 2 com 4 conexões 100GbE	2	Nó 2 com 4 conexões 100GbE
3	Nó 3 com 4 conexões 100GbE	3	Nó 3 com 4 conexões 100GbE
4	Nó 4x100GbE	4	Nó 4x100GbE
5	Nó 5 com 4 conexões 100GbE	5	Nó 5 com 4 conexões 100GbE
6	Nó 6 com 4 conexões 100GbE	6	Nó 6 com 4 conexões 100GbE
7	Nó 7 com 4 conexões 100GbE	7	Nó 7 com 4 conexões 100GbE
8	Nó 8 com 4 conexões 100GbE	8	Nó 8 com 4 conexões 100GbE
9	Nó 9 com 4 conexões 100GbE	9	Nó 9 com 4 conexões 100GbE
10	Nó 10 com 4 conexões 100GbE	10	Nó 10 com 4 conexões 100GbE
11	Nó 11 com 4 conexões 100GbE	11	Nó 11 com 4 conexões 100GbE
12	Nó 12 com 4 conexões 100GbE	12	Nó 12 com 4 conexões 100GbE
13	Nó 13 com 4 conexões 100GbE	13	Nó 13 com 4 conexões 100GbE
14	Nó 14 com 4 conexões 100GbE	14	Nó 14 com 4 conexões 100GbE
15	Nó 15 com 4 conexões 100GbE	15	Nó 15 com 4 conexões 100GbE
16	Nó 16 com 4 conexões 100GbE	16	Nó 16 com 4 conexões 100GbE
17	Nó 17 com 4 conexões 100GbE	17	Nó 17 com 4 conexões 100GbE
18	Nó 18 com 4 conexões 100GbE	18	Nó 18 com 4 conexões 100GbE
19	Nó 19 com 4 conexões 100GbE	19	Nó 19 com 4 conexões 100GbE
20	Nó 20 com 4 portas 100GbE	20	Nó 20 com 4 portas 100GbE
21	Nó 21 com 4 conexões 100GbE	21	Nó 21 com 4 conexões 100GbE
22	Nó 22 com 4 conexões 100GbE	22	Nó 22 com 4 conexões 100GbE
23	Nó 23 com 4 conexões 100GbE	23	Nó 23 com 4 conexões 100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
24	Nó 24 com 4 conexões 100GbE	24	Nó 24 com 4 conexões 100GbE
25	Nó 25 com 4 conexões 100GbE	25	Nó 25 com 4 conexões 100GbE
26	Nó 26 com 4 conexões 100GbE	26	Nó 26 com 4 conexões 100GbE
27	Nó 27 com 4 conexões 100GbE	27	Nó 27 com 4 conexões 100GbE
28	Nó 28 com 4 conexões 100GbE	28	Nó 28 com 4 conexões 100GbE
29	Nó 29 com 4 conexões 100GbE	29	Nó 29 com 4 conexões 100GbE
30	Nó 30 com 4 portas 100GbE	30	Nó 30 com 4 portas 100GbE
31	Nó 31 com 4 conexões 100GbE	31	Nó 31 com 4 conexões 100GbE
32	Nó 32 com 4 portas 100GbE	32	Nó 32 com 4 portas 100GbE
33	Nó 33 com 4 conexões 100GbE	33	Nó 33 com 4 conexões 100GbE
30	Nó 30 com 4 portas 100GbE	30	Nó 33 com 4 conexões 100GbE
34	Nó 34 com 4 conexões 100GbE	34	Nó 34 com 4 conexões 100GbE
35	Nó 35 com 4 conexões 100GbE	35	Nó 35 com 4 conexões 100GbE
36	Nó 36 com 4 conexões 100GbE	36	Nó 36 com 4 conexões 100GbE

Folha de trabalho de cabeamento em branco 9336C-FX2

Você pode usar a planilha de cabeamento em branco para documentar as plataformas suportadas como nós em um cluster. A seção *Conexões de Cluster Suportadas* do "[Hardware Universe](#)" define as portas de cluster usadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
1		1	
2		2	
3		3	
4		4	

Chave seletora de cluster A		Chave seletora de cluster B	
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	

Chave seletora de cluster A		Chave seletora de cluster B	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

Folha de exemplo de cabeamento 9336C-FX2-T (12 portas)

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 1 com 4 conexões 100GbE	1	Nó 1 com 4 conexões 100GbE
2	Nó 2 com 4 conexões 100GbE	2	Nó 2 com 4 conexões 100GbE
3	Nó 3 com 4 conexões 100GbE	3	Nó 3 com 4 conexões 100GbE
4	Nó 4x100GbE	4	Nó 4x100GbE
5	Nó 5 com 4 conexões 100GbE	5	Nó 5 com 4 conexões 100GbE
6	Nó 6 com 4 conexões 100GbE	6	Nó 6 com 4 conexões 100GbE
7	Nó 7 com 4 conexões 100GbE	7	Nó 7 com 4 conexões 100GbE
8	Nó 8 com 4 conexões 100GbE	8	Nó 8 com 4 conexões 100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
9	Nó 9 com 4 conexões 100GbE	9	Nó 9 com 4 conexões 100GbE
10	Nó 10 com 4 conexões 100GbE	10	Nó 10 com 4 conexões 100GbE
11 a 36	Requer licença	11 a 36	Requer licença

Folha de trabalho de cabeamento em branco 9336C-FX2-T (12 portas)

Você pode usar a planilha de cabeamento em branco para documentar as plataformas que são suportadas como nós em um cluster.

Chave seletora de cluster A		Chave seletora de cluster B	
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 de switch.

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você pode ["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 ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do arquivo de configuração de referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#).
- RCFs aplicáveis da rede de storage e da rede de gerenciamento da NetApp baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#).

Todos os switches de rede de storage e de gerenciamento da Cisco chegam com a configuração padrão de fábrica da Cisco. Esses switches também possuem a versão atual do software NX-OS, mas não têm os RCFs carregados.

- Documentação necessária para o switch. Consulte ["Documentação necessária"](#) para obter mais informações.

Passos

1. Instale no rack os switches de rede, switches de rede de gerenciamento e controladores.

Se você estiver instalando seu...	Então...
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte "Instalar switch em rack NetApp" para obter instruções sobre como instalar o switch em um NetApp cabinet.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches de rede e de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue a rede, os switches de rede de gerenciamento e os controladores.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp"](#). Caso contrário, acesse ["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 ter o seguinte:

- Para cada interruptor, você deve fornecer os oito parafusos 10-32 ou 12-24 e as porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiro e traseiro do gabinete.

- Você deve usar o kit de trilhos padrão da Cisco para instalar o switch em um gabinete NetApp .



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Documentação necessária

Analise os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança em "[Guia de Instalação de Hardware da Série Cisco Nexus 9000](#)".

Passos

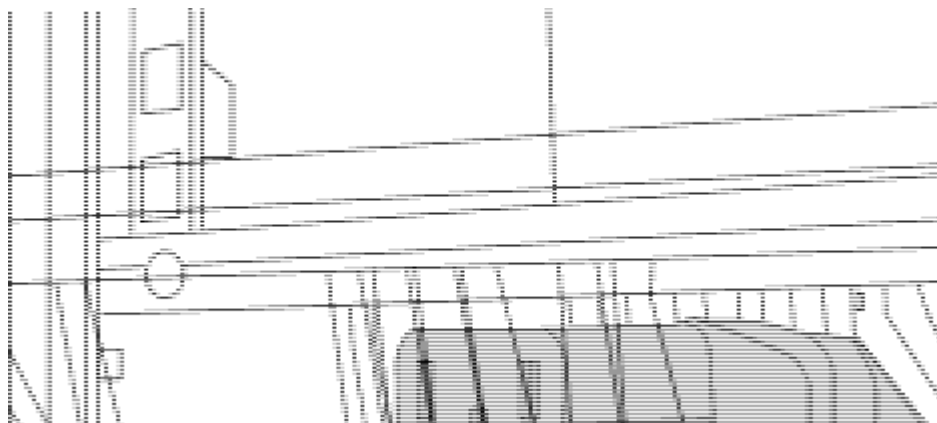
1. Instale o painel de vedação de passagem no gabinete NetApp .

O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

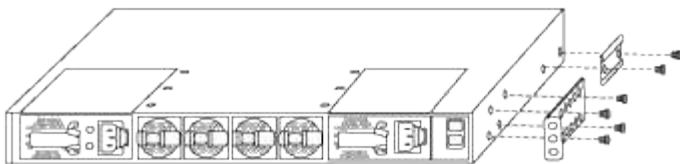
- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
 - i. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - ii. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - iii. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - iv. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.

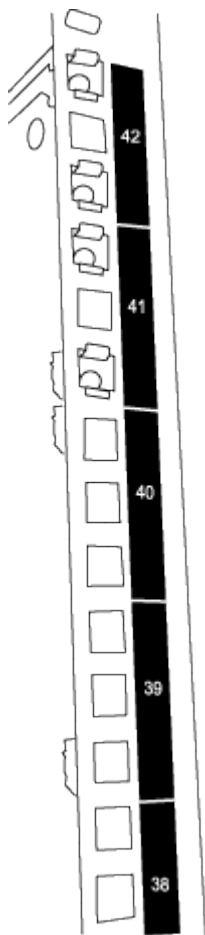


(1) Conector fêmea do cabo jumper.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.

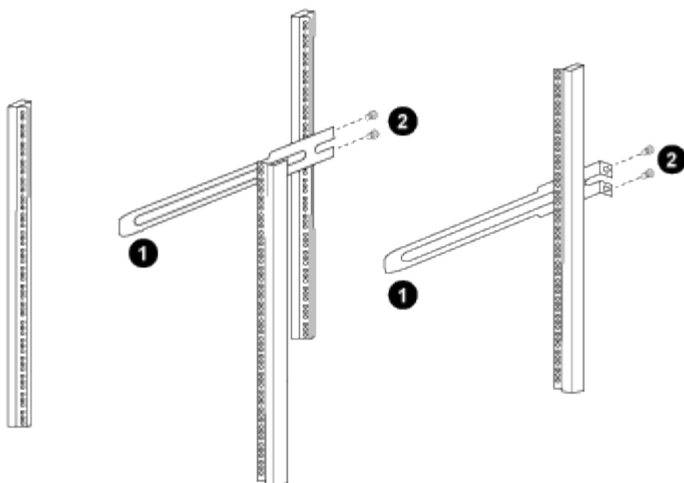


- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
3. Instale as porcas de clipe nos locais dos furos quadrados para todos os quatro postes IEA.



Os dois switches 9336C-FX2 sempre serão montados no 2U superior do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no armário.
 - a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os com os dedos.



(1) Ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos na cremalheira.

(2) Aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

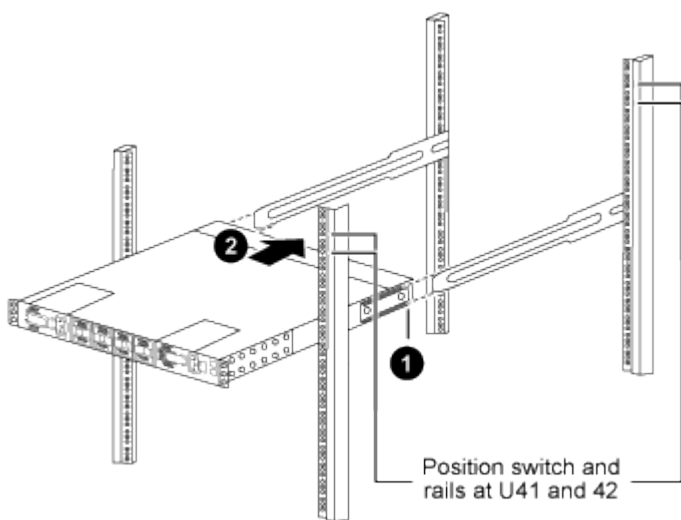
- a. Repita o passo 4a para o poste traseiro do lado direito.
- b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

5. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

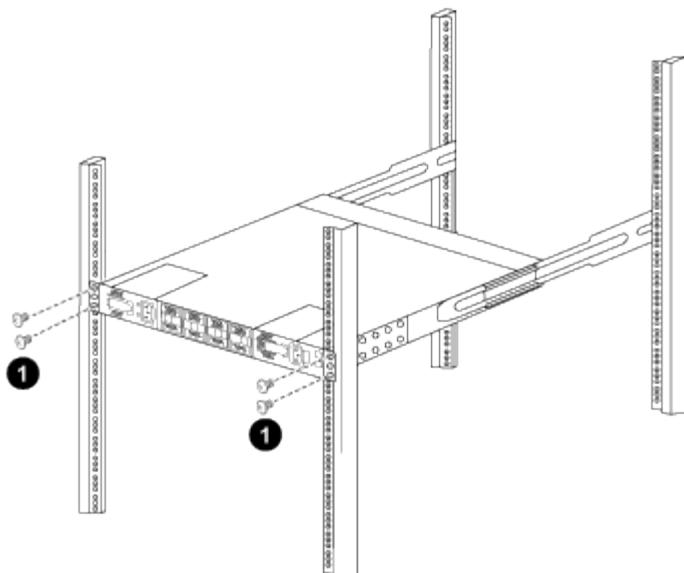
- a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

- b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

- a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos postes.
- b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

6. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
7. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

8. Conecte a porta de gerenciamento em cada switch 9336C-FX2 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

O que vem a seguir

Após instalar os switches no gabinete NetApp, você pode [configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T](#).

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seus 9336C-FX2 e 9336C-FX2-T switches, revise os requisitos de cabeamento e configuração.

Suporte para portas Ethernet NVIDIA CX6, CX6-DX e CX7.

Se você estiver conectando uma porta do switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir manualmente a velocidade da porta do switch.

```
(s1)(config)# interface Ethernet1/19
For 100GbE speed:
(s1)(config-if)# speed 100000
For 40GbE speed:
(s1)(config-if)# speed 40000
(s1)(config-if)# no negotiate auto
(s1)(config-if)# exit
(s1)(config)# exit
Save the changes:
(s1)# copy running-config startup-config
```

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

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 interruptor"

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 SSH"

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

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 ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do arquivo de configuração de referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#).
- RCFs aplicáveis de rede NetApp e de rede de gerenciamento baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#). Todos os switches de rede e de gerenciamento da Cisco chegam com a configuração padrão de fábrica da Cisco. Esses switches também possuem a versão atual do software NX-OS, mas não têm os RCFs carregados.
- Documentação necessária para o switch. Consulte ["Documentação necessária"](#) para obter mais informações.

Passos

1. Realize uma configuração inicial dos switches de rede.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.

Incitar	Resposta
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	O nome do interruptor está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave, de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.

Incitar	Resposta
Configurar camada de interface padrão (L3/L2)	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado)	Responda com noshut . O padrão é noshut.
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso)	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

2. Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
3. Verifique a versão nos switches de rede e, se necessário, baixe a versão do software compatível com a NetApp para os switches na página ["Download do software Cisco"](#).

O que vem a seguir?

Depois de configurar seus switches, você pode ["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 Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são s1 e s2.
- Os nomes dos nós são cluster1-01 e cluster1-02.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Se AutoSupport estiver ativado, suprima a criação automática de casos enviando uma mensagem
AutoSupport: system node autosupport invoke -node * -type all -message MAINT=xh
onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

3. Exibir quantas interfaces estão configuradas em cada nó para cada switch:

```
network device-discovery show -protocol lldp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/lldp				
	e5a	s1	Eth1/2	N9K-
C9336C				
	e3b	s2	Eth1/2	N9K-
C9336C				
cluster1-01/lldp				
	e5a	s1	Eth1/1	N9K-
C9336C				
	e3b	s2	Eth1/1	N9K-
C9336C				
.				
.				

4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.

a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
Speed                               VLAN
Node                               Port Type Mode   (Gb/s) State   Status   ID
-----
cluster1-01
      e5a  ENET  storage  100 enabled online   -
      e3b  ENET  storage  100 enabled online   -
cluster1-02
      e5a  ENET  storage  100 enabled online   -
      e3b  ENET  storage  100 enabled online   -
.
.
```

b. Exiba os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show

Shelf ID Module State           Internal?
-----
1.4
      0 A      connected false
      1 A      connected false
      2 B      connected false
      3 B      connected false
.
.
```

c. Verifique se o monitoramento de integridade do switch (CSHM) está ativado para o switch para que os switches sejam monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	1.2.3.4	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX1			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			
s2	storage-network	2.3.4.5	N9K-
C9336C-FX2			
Serial Number: FEEXXXXXXX2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			

O que vem a seguir?

Após preparar a instalação do software NX-OS e do RCF, você pode ["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 Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar, conclua o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) .

Requisitos de revisão

Antes de começar

Certifique-se de ter 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 da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornece informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são s1 e s2.
- Os nomes dos nós são cluster1-01 e cluster1-02.

Instale ou atualize o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Conecte o switch à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue alcançar o servidor no endereço IP 172.19.2.1:

```
s2# 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. Se você estiver configurando seu switch pela primeira vez, pule para a etapa 5. Se estiver atualizando seu switch, prossiga para a próxima etapa.
4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.

- a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
Speed                               VLAN
Node                               Mode    (Gb/s)  State   Status   ID
-----
cluster1-01
      e5a  ENET  storage    100 enabled  online   -
      e3b  ENET  storage    100 enabled  online   -
cluster1-02
      e5a  ENET  storage    100 enabled  online   -
      e3b  ENET  storage    100 enabled  online   -
.
.
```

- b. Exiba os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show

Shelf ID Module State           Internal?
-----
1.4
    0 A      connected    false
    1 A      connected    false
    2 B      connected    false
    3 B      connected    false
.
.
```

- c. Verifique se o monitoramento de integridade do switch (CSHM) está ativado para o switch para que os switches sejam monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	1.2.3.4	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX1			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			
s2	storage-network	2.3.4.5	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			

5. Faça login no switch usando SSH ou usando um console serial.
6. Copie o software NX-OS e as imagens EPLD para o switch Nexus 9336C-FX2.

Mostrar exemplo

```
s2# 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.

s2# 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 do software NX-OS em execução:

```
show version
```

Mostrar exemplo

```
s2# 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: s2
  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):
```

8. Instale a imagem do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

Mostrar exemplo

```
s2# 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 após a reinicialização do switch:

```
show version
```

Mostrar exemplo

```
s2# 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: s2
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



s2# **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

s2# **install epld bootflash:n9000-epld.9.3.5.img module all**

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

```
s2# 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. Se você estiver configurando seu switch pela primeira vez, pule para a etapa 14. Se você estiver atualizando seu switch, prossiga para a próxima etapa.
13. Verifique o status de integridade de cada porta de storage do nó e de cada porta de storage shelf.
- a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
```

Speed	VLAN						
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
-----	----	-----	-----	-----	-----	-----	----
cluster1-01							
	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-
cluster1-02							
	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-
.							
.							

- b. Exiba os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- c. Verifique se o monitoramento de integridade do switch (CSHM) está habilitado para os switches para que eles sejam monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	1.2.3.4	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX1			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			
s2	storage-network	2.3.4.5	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			

14. Repita os passos 5 a 13 para instalar o software NX-OS no switch s1.

O que vem a seguir?

Após instalar ou atualizar o software NX-OS, você pode ["instalar ou atualizar o RCF"](#) .

Instale ou atualize o RCF

Visão geral da instalação ou atualização do Arquivo de Configuração de Referência (RCF)

Você instala o Arquivo de Configuração de Referência (RCF) após configurar o switch de armazenamento Nexus 9336C-FX2 pela primeira vez. Você atualiza sua versão RCF quando tem uma versão existente do arquivo RCF instalada no seu switch.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configuração RCF disponível

Storage - (Storage RCF 1.xx) é a configuração RCF disponível onde todas as portas estão configuradas para conexões de storage NVMe de 100GbE.

Documentação sugerida

- ["Switches Ethernet da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 9000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são s1 e s2.
- Os nomes dos nós são cluster1-01 e cluster1-02.

Consulte o ["Hardware Universe"](#) para verificar as portas corretas em sua plataforma.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

O que vem a seguir?

Após revisar o procedimento de instalação ou atualização do RCF, você pode ["instalar o RCF"](#) ou ["atualize seu RCF"](#) Conforme necessário.

Instale o arquivo 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 Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar seu RCF.

Antes de começar

Verifique as seguintes instalações e conexões:

- Uma conexão de console com o switch. A conexão com o console é opcional se você tiver acesso remoto ao switch.
- Os switches s1 e s2 estão ligados e a configuração inicial dos switches está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão desejada do NX-OS foi instalada.
- As portas de armazenamento do nó ONTAP e as portas do compartimento de armazenamento não estão conectadas.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch s2 usando SSH ou usando um console serial.
2. Copie o RCF para a bootflash do switch s2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um RCF para a bootflash no switch s2:

```
s2# copy tftp: bootflash: vrf management
Enter source filename: NX9336C-FX2-RCF-v1.13-1-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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o RCF NX9336C-FX2-RCF-v1.13-1-Storage.txt sendo instalado no switch s2:

```
s2# copy NX9336C-FX2-RCF-v1.13-1-Storage.txt running-config echo-
commands
```

4. Examine a saída do banner do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e o funcionamento corretos do switch.

Mostrar exemplo

```
s2# show banner motd

*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : NX9336C-FX2
* Filename    : NX9336C-FX2-RCF-v1.13-1-Storage.txt
* Date        : 05-22-2025
* Version     : v1.13
*
* Port Usage  : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*
* IMPORTANT NOTES
*
* Interface port-channel999 is reserved to identify the version of
this file.
*****
```

5. Verifique se o RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.

7. Após verificar se as versões do RCF e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

```
s2# copy running-config startup-config
[#####] 100% Copy complete
```

8. Reinicie o switch s2.

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

9. Repita as etapas de 1 a 8 no switch s1.
10. Conecte as portas de armazenamento dos nós e as portas dos gabinetes de armazenamento de todos os nós no cluster ONTAP aos switches s1 e s2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch estão **up**.

```
show interface brief
```


Mostrar exemplo

```
s1# 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 as portas de storage do nó e as portas do shelf de storage estão nas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
s1# 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

```
s1# show interface trunk
```

Port	Native Vlan	Status	Port 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 sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

Etapas 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager oferece um fluxo de trabalho simples e fácil para a configuração e instalação de clusters, incluindo a atribuição de um endereço IP de gerenciamento de nó, a inicialização do cluster, a criação de uma camada local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Vá para ["Configurar o ONTAP em um novo cluster com o System Manager"](#) Para obter instruções de configuração.

O que vem a seguir?

Após instalar o seu RCF, você pode ["verificar a configuração SSH"](#)

Atualize seu Arquivo de Configuração de Referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapas 1: Prepare-se para a atualização

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


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

Onde x representa a duração do período de manutenção em horas.

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

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exiba as portas em cada nó que estão conectadas aos switches:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID) Interface      Platform
-----
-----
cluster1-01/cdp
           e5a    s1                Ethernet1/7    N9K-
C9336C
           e3b    s2                Ethernet1/7    N9K-
C9336C
cluster1-02/cdp
           e5a    s1                Ethernet1/8    N9K-
C9336C
           e3b    s2                Ethernet1/8    N9K-
C9336C
.
.
.
```

4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.

- a. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- b. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- c. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::*> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	1.2.3.4	N9K-
C9336C-FX2			
Serial Number: FFFXXXXXXX1			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			
s2	storage-network	2.3.4.5	N9K-
C9336C-FX2			
Serial Number: FEEXXXXXXX2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			

Etapa 2: atualize o RCF

1. Faça login no switch s2 usando SSH ou usando um console serial.
2. Desligue as portas conectadas a todas as portas dos nós.

```
s2> enable  
s2# configure  
s2(config)# interface e1/1-36  
s2(config-if-range)# shutdown  
s2(config-if-range)# exit  
s2(config)# exit
```



Certifique-se de desativar **todas** as portas conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) para obter mais detalhes.

3. Caso ainda não o tenha feito, 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 versões posteriores, use o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, utilize uma ferramenta de comparação ou de diferenças de terceiros.
4. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
s2# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
s2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
s2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
s2# show run | section "switchname" >> bootflash:write_erase.cfg
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

5. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

6. Emita o `write erase` comando para apagar a configuração salva atual:

```
s2# 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 para a configuração de inicialização.

```
s2# copy bootflash:write_erase.cfg startup-config
```

8. Reinicie o switch:

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

9. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

10. Copie o RCF para a bootflash do switch s2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um RCF para a bootflash no switch s2:

```
s2# copy tftp: bootflash: vrf management
Enter source filename: NX9336C-FX2-RCF-v1.13-1-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)...
```

11. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Este exemplo mostra o arquivo RCF NX9336C-FX2-RCF-v1.13-1-Storage.txt sendo instalado no switch s2:

```
s2# copy NX9336C-FX2-RCF-v1.13-1-Storage.txt running-config echo-
commands
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

12. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e

consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

13. Reaplique quaisquer personalizações anteriores à configuração do switch.
14. Após verificar se as versões do RCF, as adições personalizadas e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

```
s2# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

15. Reinicialize o switch s2. Você pode ignorar os alertas do "monitor de integridade do switch do cluster" e os eventos de "portas do cluster inativas" relatados nos nós enquanto o switch reinicializa.

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

16. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.
 - a. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- b. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

c. Verifique se os switches estão sendo monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
Switch          Type          Address          Model
-----
s1              storage-network  1.2.3.4          N9K-
C9336C-FX2
  Serial Number: FFFXXXXXXX1
  Is Monitored: true
    Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  10.3(4a)
  Version Source: CDP/ISDP
s2              storage-network  2.3.4.5          N9K-
C9336C-FX2
  Serial Number: FEEXXXXXXX2
  Is Monitored: true
    Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  10.3(4a)
  Version Source: CDP/ISDP
```

17. Repita as etapas de 1 a 16 no switch s1.

Etapa 3: verifique a rede de storage

Conclua as seguintes etapas em cada switch de storage para verificar se a rede de storage está funcionando corretamente após a atualização do RCF.

1. Verifique se as portas do switch conectadas às portas de storage do nó e às portas do shelf de storage estão **up**.

```
show interface brief
```

2. Verifique se as portas de storage do nó esperadas ainda estão conectadas:

```
show cdp neighbors
```

3. Verifique se as portas esperadas do compartimento de storage ainda estão conectadas:


```
show lldp neighbors
```

4. Verifique se as portas de storage do nó e as portas do shelf de storage estão nas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

O que vem a seguir?

Após atualizar seu RCF, você pode ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches.

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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer           1          enabled
(switch)#
```



Ao habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Consulte ["Configure a segurança de rede usando FIPS."](#) para mais detalhes.

O que vem a seguir?

Após 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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

Passos

1. Apagar a configuração existente:

```
write erase
```

```
(s2) # 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
```

```
(s2) # 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.

O que vem a seguir

Depois de reiniciar os interruptores, você pode [reconfigurar](#) eles conforme necessário.

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 de switches na página de switches Ethernet da Cisco para obter informações sobre as versões suportadas do ONTAP, NX-OS e RCF.
- Você consultou os guias de software e atualização apropriados disponíveis no site da Cisco .
- Você baixou os RCFs aplicáveis.
- A configuração de rede existente apresenta as seguintes características:
 - A página de switches Ethernet da Cisco contém as versões mais recentes do RCF e do NX-OS para seus switches.
 - A conectividade de gerenciamento deve existir em ambos os switches.
- O switch Cisco Nexus 9336C-FX2 de substituição possui as seguintes características:
 - A conectividade da rede de gerenciamento está funcional.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - A imagem apropriada do sistema operacional RCF e NX-OS é carregada no switch.
 - A configuração inicial do switch está concluída.

Sobre esta tarefa

Este procedimento substitui o segundo switch de storage Nexus 9336C-FX2 s2 pelo novo switch 9336C-FX ns2. Os dois nós são cluster1-01 e cluster1-02.

Passos para concluir:

- Confirme se o switch a ser substituído é s2.
- Desconecte os cabos do switch s2.
- Reconecte os cabos ao switch ns2.
- Verifique todas as configurações do dispositivo no switch ns2.



Pode haver dependências entre a sintaxe de comandos nas versões RCF e NX-OS.

Passos

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

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

x representa a duração da janela de manutenção em horas.

2. Verifique o status de integridade das portas do nó de storage para garantir que há conexão com o switch de storage s1:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
cluster1-01	e5a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
cluster1-02	e5a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
.							
.							

3. Verifique se o switch de storage s1 está disponível:

```
network device-discovery show
```

Mostrar exemplo

```
storage::*> network device-discovery show
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
cluster1-01/cdp				
	e5a	s1	Ethernet1/1	NX9336C
	e4a	cluster1-02	e4a	AFF-A700
	e4e	cluster1-02	e4e	AFF-A700
cluster1-01/lldp				
	e5a	s1	Ethernet1/1	-
	e4a	cluster1-02	e4a	-
	e4e	cluster1-02	e4e	-
cluster1-02/cdp				
	e3b	s1	Ethernet1/2	NX9336C
	e4a	cluster1-01	e4a	AFF-A700
	e4e	cluster1-01	e4e	AFF-A700
cluster1-02/lldp				
	e3b	s1	Ethernet1/2	-
	e4a	cluster1-01	e4a	-
	e4e	cluster1-01	e4e	-
.				
.				

4. Comande o espetáculo `lldp neighbors` Execute o comando no switch em funcionamento para confirmar que você consegue visualizar ambos os nós e todas as prateleiras:

```
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
cluster1-01        Eth1/1      121         S            e5a
cluster1-02        Eth1/2      121         S            e5a
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 das prateleiras de armazenamento 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  -            -
.
.
```

6. Remova todos os cabos conectados ao switch de storage s2.
7. Reconecte todos os cabos ao switch de substituição ns2.
8. Verifique novamente o estado de integridade das portas do nó de armazenamento:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
cluster1-01	e5a	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
cluster1-02	e5a	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
.							
.							

9. Verifique se ambos os interruptores estão disponíveis:

```
network device-discovery show
```

Mostrar exemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----
cluster1-01/cdp
    e3a  s1                Ethernet1/1 NX9336C
    e4a  cluster1-02        e4a         AFF-A700
    e4e  cluster1-02        e4e         AFF-A700
    e7b  ns2                Ethernet1/1 NX9336C
cluster1-01/lldp
    e3a  s1                Ethernet1/1 -
    e4a  cluster1-02        e4a         -
    e4e  cluster1-02        e4e         -
    e7b  ns2                Ethernet1/1 -
cluster1-02/cdp
    e3a  s1                Ethernet1/2 NX9336C
    e4a  cluster1-01        e4a         AFF-A700
    e4e  cluster1-01        e4e         AFF-A700
    e7b  ns2                Ethernet1/2 NX9336C
cluster1-02/lldp
    e3a  s1                Ethernet1/2 -
    e4a  cluster1-01        e4a         -
    e4e  cluster1-01        e4e         -
    e7b  ns2                Ethernet1/2 -
.
.
```

10. Verifique as portas das prateleiras no sistema de armazenamento:

```
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 desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Cisco Nexus 3232C

Começar

Fluxo de trabalho de instalação e configuração para switches de armazenamento Cisco Nexus 3232C

Os switches Cisco Nexus 3232C fazem parte da plataforma Cisco Nexus 3000 e podem ser instalados em um gabinete de sistema NetApp.

Siga estes passos do fluxo de trabalho para instalar e configurar seus switches Cisco 3232C.

1

"Revise os requisitos de configuração"

Analise os requisitos de configuração para os switches de armazenamento 3232C.

2

"Revise a documentação necessária"

Revise a documentação específica do switch e do controlador para configurar seus switches 3232C e o cluster ONTAP .

3

"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.



"Instale o hardware"

Instale o hardware do switch.



"Configurar o software"

Configure o software do switch.

Requisitos de configuração para switches de armazenamento Cisco Nexus 3232C

Para instalação e manutenção do switch Cisco Nexus 3232C, certifique-se de revisar os requisitos de configuração e de rede.

Requisitos de configuração

Você precisa da quantidade e do tipo adequados de cabos e conectores para seus switches. Dependendo do tipo de switch que você estiver configurando inicialmente, você precisa conectar à porta de console do switch com o cabo de console incluso; você também precisa fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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 o ["Hardware Universe"](#) Para obter as informações mais recentes. Ver ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) Para obter mais informações sobre os requisitos de instalação do switch.

O que vem a seguir

Após confirmar seus requisitos de configuração, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches de armazenamento Cisco Nexus 3232C

Para a instalação do switch Cisco Nexus 3232C, certifique-se de revisar toda a documentação recomendada.

Documentação do Switch

Para configurar os switches Cisco Nexus 3232C, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 3000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 3000</i>	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 3000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 3000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 3000 Series NX-OS</i>	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 3000</i>	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 3000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 3000</i>	Descreve as mensagens do sistema para switches da série Cisco Nexus 3000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de versão do NX-OS para a série Cisco Nexus 3000 (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 3000.
Informações regulamentares, de conformidade e de segurança para os Cisco Nexus 6000, Cisco Nexus série 5000, Cisco Nexus série 3000 e Cisco Nexus série 2000.	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 3000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornecer informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco 3232C em um gabinete NetApp , consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"Instale um switch Cisco Nexus 3232C em um gabinete NetApp ."	Este manual descreve como instalar um switch Cisco Nexus 3232C em um gabinete NetApp de quatro postes.

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar hardware

Fluxo de trabalho de instalação de hardware para switches Cisco Nexus 3232C

Para instalar e configurar o hardware de um switch de armazenamento 3232C, siga estas etapas:

1

"Instale o interruptor"

Instale o switch de armazenamento 3232C.

2

"Instale o switch em um gabinete NetApp ."

Instale o switch de armazenamento 3232C e o painel de passagem em um gabinete NetApp conforme necessário.

3

"Analise as considerações sobre cabeamento e configuração."

Revise as considerações de cabeamento e configuração para o switch de storage 3232C.

Instale o switch de armazenamento 3232C

Siga este procedimento para configurar o switch de armazenamento Cisco Nexus 3232C.

Antes de começar

Certifique-se de ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) . Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando o...	Então...
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia _Instalação de um switch de cluster Cisco Nexus 3232C e painel de passagem em um gabinete NetApp para obter instruções sobre como instalar o switch em um gabinete NetApp .

Se você estiver instalando o...	Então...
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação de hardware do switch e nas instruções de instalação e configuração da NetApp .

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.

O que vem a seguir?

Após instalar o switch de armazenamento 3232C, você pode então ["instale o switch em um NetApp cabinet"](#).

Instale um switch de armazenamento Cisco Nexus 3232C em um gabinete NetApp

Dependendo da sua configuração, pode ser necessário instalar o switch de armazenamento Cisco Nexus 3232C e o painel de passagem em um NetApp cabinet com os suportes padrão que acompanham o switch.

Antes de começar

Verifique se você possui o seguinte: * Os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança no ["Guia de Instalação de Hardware da Série Cisco Nexus 3000"](#). * Para cada switch, os oito parafusos 10-32 ou 12-24 e as porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiro e traseiro do gabinete. * Kit de trilhos padrão Cisco para instalar o switch em um gabinete NetApp.



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Passos

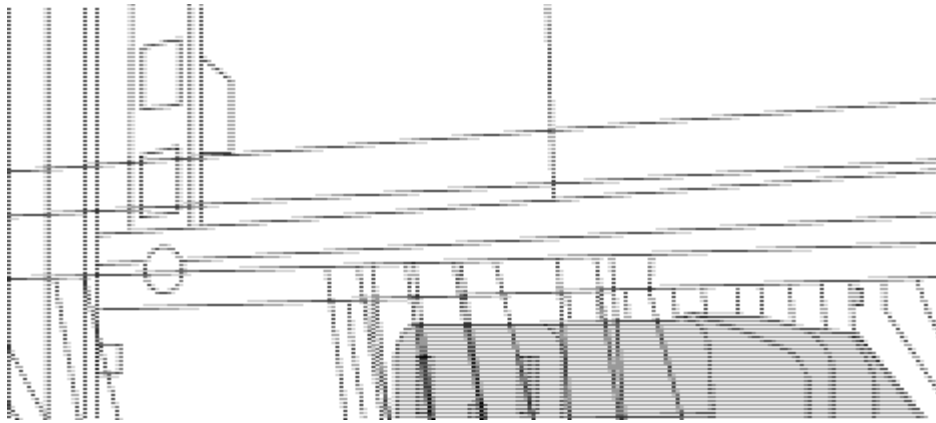
1. Instale o painel de vedação de passagem no gabinete NetApp .

O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

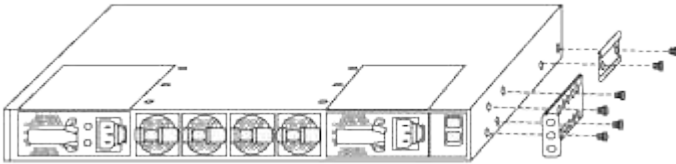
- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
 - i. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - ii. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - iii. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - iv. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.

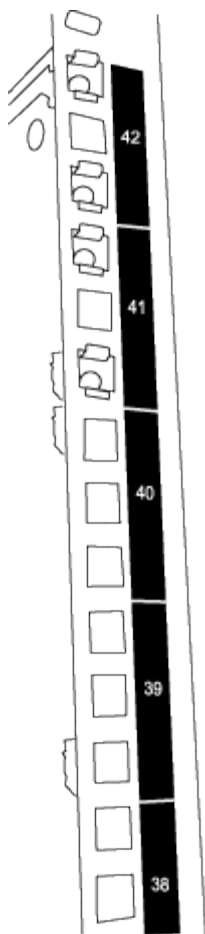


(1) Conector fêmea do cabo jumper.

1. Instale os suportes de montagem em rack no chassi do switch de armazenamento Nexus 3232C.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.



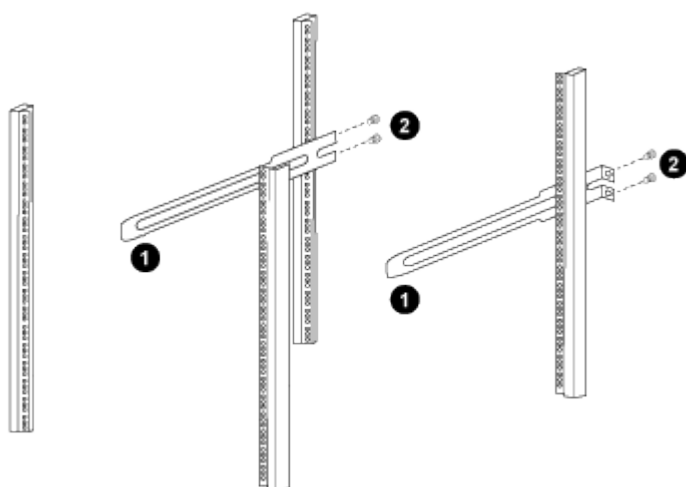
- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
2. Instale as porcas de clipe nos locais dos furos quadrados para todos os quatro postes IEA.



Os dois switches 3232C sempre serão montados no 2U superior do gabinete RU41 e 42.

3. Instale os trilhos deslizantes no armário.

- a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os 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 o poste traseiro do lado direito.

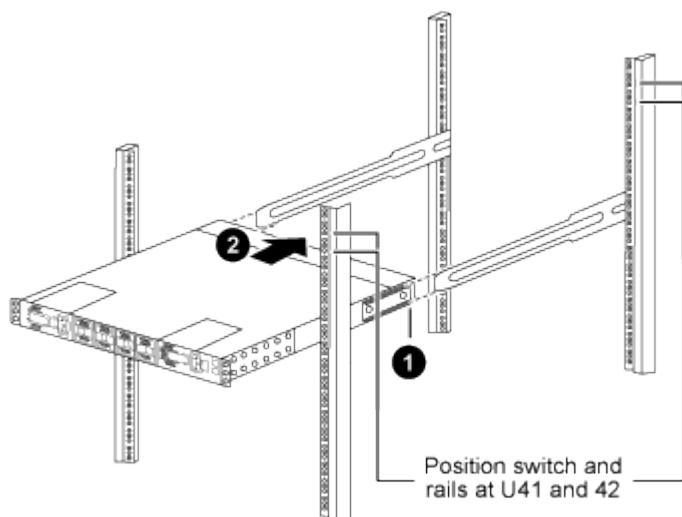
b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

4. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

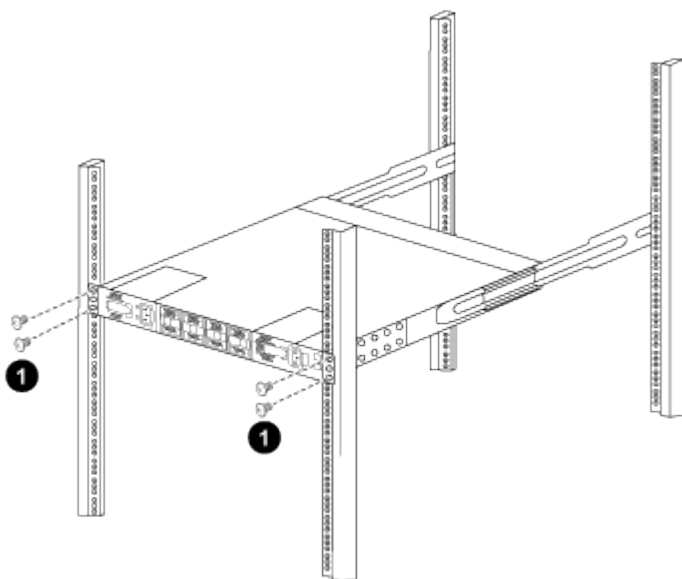
a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos

postes.

b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

5. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
6. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

7. Conecte a porta de gerenciamento em cada switch 3232C 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seus switches 3232C, revise os requisitos de cabeamento e configuração.

Suporte para portas Ethernet NVIDIA CX6, CX6-DX e CX7.

Se você estiver conectando uma porta do switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir manualmente a velocidade da porta do switch.

```
(s1)(config)# interface Ethernet1/19
For 100GbE speed:
(s1)(config-if)# speed 100000
For 40GbE speed:
(s1)(config-if)# speed 40000
(s1)(config-if)# no negotiate auto
(s1)(config-if)# exit
(s1)(config)# exit
Save the changes:
(s1)# copy running-config startup-config
```

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Configurar software

Fluxo de trabalho de instalação de software para switches de armazenamento 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 interruptor"

Configurar o switch de armazenamento 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 armazenamento Cisco 3232C.

3

"Instale ou atualize o software NX-OS."

Faça o download, instale ou atualize o software NX-OS no switch de armazenamento Cisco 3232C.

4

"Instale o RCF"

Instale o RCF após configurar o switch de armazenamento Cisco 3232C pela primeira vez.

5

"Atualize o RCF"

Atualize sua versão existente do RCF conforme necessário.

6

"Verifique a configuração SSH"

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

Configurar o switch de armazenamento 3232C

Siga este procedimento para instalar e configurar o switch Cisco Nexus 3232C.

Antes de começar

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do arquivo de configuração de referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Documentação necessária sobre a rede e o switch de gerenciamento de rede.

Veja ["Documentação necessária"](#) para mais informações.

- Documentação do controlador e documentação do ONTAP necessárias.

- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Arquivos RCF aplicáveis da NetApp para a rede de storage e a rede de gerenciamento, baixados do site de suporte da NetApp em "meusuporte.netapp.com" para os switches que você receber. Todos os switches de rede de storage e de rede de gerenciamento da Cisco chegam com a configuração padrão de fábrica da Cisco. Esses switches também possuem a versão atual do software NX-OS, mas não têm os RCFs carregados.

Passos

1. Instale os switches da rede de storage, da rede de gerenciamento e os controladores no rack.

Se você estiver instalando seu...	Então...
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch Cisco Nexus 3232C e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação de hardware do switch e nas instruções de instalação e configuração da NetApp .

2. Conecte os switches da rede de storage e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches da rede de storage, da rede de gerenciamento e os controladores.
4. Realize uma configuração inicial dos switches da rede de storage.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .

Incitar	Resposta
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	O nome do interruptor está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave entre 1024 e 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.
Configurar a camada de interface padrão (L3/L2):	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado):	Responda com noshut . O padrão é noshut.

Incitar	Resposta
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso):	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

- Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
- Verifique a versão nos switches de rede e, se necessário, baixe a versão do software compatível com a NetApp para os switches na página ["Download do software Cisco"](#).

O que vem a seguir?

Depois de configurar seus switches, você pode ["Prepare-se para instalar o NX-OS e o RCF"](#).

Prepare-se para instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF).

Antes de instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são s1 e s2.
- Os nomes dos nós são cluster1-01 e cluster1-02.

Veja o ["Hardware Universe"](#) para verificar as portas de rede corretas em suas plataformas. Veja ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para mais informações sobre os requisitos de instalação do switch.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

- Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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 do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

3. Exibir quantas interfaces estão configuradas em cada nó para cada switch:

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e5a	s1	Eth1/2	N3K-
C3232C	e3b	s2	Eth1/2	N3K-
C3232C				
cluster1-01/cdp	e5a	s1	Eth1/1	N3K-
C3232C	e3b	s2	Eth1/1	N3K-
C3232C				
.				
.				

4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.

- a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
```

Speed			VLAN				
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
-----	----	-----	-----	-----	-----	-----	----
cluster1-01	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-
cluster1-02							
	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-
.							
.							

- b. Exibir os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- c. Verifique se o monitoramento de integridade do switch (CSHM) está habilitado para os switches para que eles sejam monitorados:

```
system switch ethernet show
```


Mostrar exemplo

```
cluster1::> system switch ethernet show
Switch                Type                Address                Model
-----
s1                    storage-network    1.0.0.0                N3K-C3232C
  Serial Number: FFFYYYYYYY1
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    10.3(4a)
  Version Source: CDP/ISDP
s2                    storage-network    1.1.0.0                N3K-C3232C
  Serial Number: FEEYYYYYYY2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    10.3(4a)
  Version Source: CDP/ISDP
```

O que vem a seguir?

Depois de se preparar para instalar o software NX-OS e o RCF, você pode ["Instale o software NX-OS."](#)

Instale ou atualize o software NX-OS.

Você pode usar este procedimento para instalar o software NX-OS no switch de armazenamento Nexus 3232C.

Antes de começar

Verifique se você possui o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- ["Página do switch Ethernet da Cisco"](#). Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do NX-OS.
- ["Switches Cisco Nexus série 3000"](#). 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 dos switches Cisco .

Instale ou atualize o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os

comandos ONTAP são usados, a menos que indicado de outra forma.

Conclua o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) e depois siga os passos abaixo.

Passos

1. Conecte o switch à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue alcançar o servidor no endereço IP 172.19.2.1:

```
s2# 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. Se você estiver configurando seu switch pela primeira vez, pule para a etapa 5. Se estiver atualizando seu switch, prossiga para a próxima etapa.
4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.

- a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
Speed                               VLAN
Node                               Port Type Mode   (Gb/s) State   Status   ID
-----
cluster1-01
      e5a  ENET  storage  100 enabled online   -
      e3b  ENET  storage  100 enabled online   -
cluster1-02
      e5a  ENET  storage  100 enabled online   -
      e3b  ENET  storage  100 enabled online   -
.
.
```

- b. Exibir os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
Shelf ID Module State          Internal?
----- --
1.4
    0 A      connected         false
    1 A      connected         false
    2 B      connected         false
    3 B      connected         false
.
.
```

- c. Verifique se o monitoramento de integridade do switch (CSHM) está habilitado para os switches para que eles sejam monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
Switch          Type          Address          Model
-----
s1              storage-network 1.0.0.0          N3K-C3232C
  Serial Number: FFFYYYYYYY1
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  10.3(4a)
  Version Source: CDP/ISDP
s2              storage-network 1.1.0.0          N3K-C3232C
  Serial Number: FEEYYYYYYY2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  10.3(4a)
  Version Source: CDP/ISDP
```

5. Faça login no switch usando SSH ou usando um console serial.
6. Copie o software NX-OS e as imagens EPLD para o switch Nexus 3232C.

Mostrar exemplo

```
s2# 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.

s2# 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 do software NX-OS em execução:

```
show version
```

Mostrar exemplo

```
s2# 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: s2
  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):
```

8. Instale a imagem do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

Mostrar exemplo

```
s2# 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.
```

9. Verifique a nova versão do software NX-OS após a reinicialização do switch:

```
show version
```


Mostrar exemplo

```
s2# 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):

10. Atualize a imagem EPLD e reinicie o switch.

Mostrar exemplo

```
s2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x12
IO FPGA	0x11

```
s2# 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.

11. Se você estiver atualizando para a versão 9.3(11) do NX-OS, você deve atualizar o EPLD. golden Crie a imagem e reinicie o switch mais uma vez. Caso contrário, passe para a etapa 12.

Ver "Notas de versão da atualização EPLD, versão 9.3(11)" Para obter mais detalhes.

Mostrar exemplo

```
s2# 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.
```

12. Após a reinicialização do switch, faça login para verificar se a nova versão do EPLD foi carregada com sucesso.

Mostrar exemplo

```
s2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x12
IO FPGA	0x12

13. Se você estiver configurando seu switch pela primeira vez, pule para a etapa 15. Se estiver atualizando seu switch, prossiga para a próxima etapa.
14. Verifique o status de integridade de cada porta de storage do nó e de cada porta de storage shelf.
 - a. Exiba os atributos da porta de storage do nó:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
```

Speed			VLAN				
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
cluster1-01	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-
cluster1-02	e5a	ENET	storage	100	enabled	online	-
	e3b	ENET	storage	100	enabled	online	-

- b. Exibir os atributos da porta da prateleira de storage:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::*> storage shelf port show
Shelf ID Module State          Internal?
----- --
1.4
    0 A      connected         false
    1 A      connected         false
    2 B      connected         false
    3 B      connected         false
.
.
```

- c. Verifique se o monitoramento de integridade do switch (CSHM) está habilitado para os switches para que eles sejam monitorados:

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::> system switch ethernet show
Switch          Type          Address          Model
-----
s1              storage-network 1.0.0.0          N3K-C3232C
  Serial Number: FFFYYYYYYY1
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  10.3(4a)
  Version Source: CDP/ISDP
s2              storage-network 1.1.0.0          N3K-C3232C
  Serial Number: FEEYYYYYYY2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  10.3(4a)
  Version Source: CDP/ISDP false
```

15. Repita os passos 5 a 13 para instalar o software NX-OS no switch s1.

O que vem a seguir?

Após instalar o software NX-OS, você pode ["instalar ou atualizar o arquivo de configuração de referência \(RCF\)"](#).

Instale o arquivo de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches Nexus 3232C pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual.
- Uma conexão de console com o switch, isso é necessário ao instalar o RCF.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Conclua o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) e depois siga os passos abaixo.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch s2 usando SSH ou usando um console serial.
2. Copie o RCF para a bootflash do switch s2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um RCF para a bootflash no switch s2:

```
s2# copy tftp: bootflash: vrf management
Enter source filename: NX3232C-RCF-v1.13-1-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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos Cisco , consulte o guia apropriado no ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#) .

Mostrar exemplo

Este exemplo mostra o arquivo RCF `NX9336C-FX2-RCF-v1.13-1-Storage.txt` sendo instalado no switch `s2`:

```
s2# copy NX9336C-FX2-RCF-v1.13-1-Storage.txt running-config echo-commands
```



Certifique-se de ler atentamente as seções **Installation notes**, **Important Notes** e **banner** do seu RCF. Você deve ler e seguir essas instruções para verificar a configuração e o funcionamento corretos do switch.

4. Examine a saída do banner 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.
5. Verifique se o RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Reaplique quaisquer personalizações anteriores à configuração do switch.
7. Após verificar se as versões do RCF e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

```
s2# copy running-config startup-config [] 100% Copy complete
```

8. Reinicializar o switch `s2`:

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

9. Repita as etapas 1 a 8 no switch `s1`.
10. Conecte as portas de storage dos nós e as portas dos shelves de storage de todos os nós no cluster ONTAP aos switches `s1` e `s2`.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch estão **up**.


```
show interface brief
```

2. Verifique se as portas de storage do nó e as portas do shelf de storage estão nas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Etapa 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e instalação de cluster, incluindo atribuição de um endereço IP de gerenciamento de nó, inicialização do cluster, criação de uma camada local, configuração de protocolos e provisionamento de armazenamento inicial.

Consulte "[Configurar o ONTAP em um novo cluster com o System Manager](#)" para obter instruções de configuração.

O que vem a seguir?

Após instalar o RCF, você pode "[verificar a configuração SSH](#)".

Atualize seu Arquivo de Configuração de Referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu 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, deverá fazer isso antes de reaplicar o RCF para que a versão correta seja incluída em reinicializações futuras.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapa 1: Prepare-se para a atualização

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

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

Onde x representa a duração do período de manutenção em horas.

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

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

3. Exiba as portas em cada nó que estão conectadas aos switches:

```
network device-discovery show
```

Mostrar exemplo

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID) Interface      Platform
-----
cluster1-01/cdp
              e5a    s1                Ethernet1/7    N3K-
C3232C
              e3b    s2                Ethernet1/7    N3K-
C3232C
cluster1-02/cdp
              e5a    s1                Ethernet1/8    N3K-
C3232C
              e3b    s2                Ethernet1/8    N3K-
C3232C
.
```

4. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.
 - a. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- b. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- c. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::*> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	1.2.3.4	N3K-
C3232C			
Serial Number: FFFXXXXXXX1			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			
s2	storage-network	2.3.4.5	N3K-
C3232C			
Serial Number: FEEXXXXXXX2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
10.3(4a)			
Version Source: CDP/ISDP			

Etapa 2: atualize o RCF

1. Faça login no switch s2 usando SSH ou usando um console serial.
2. Desligue as portas conectadas a todas as portas dos nós.

```
s2> enable  
s2# configure  
s2(config)# interface e1/1-32  
s2(config-if-range)# shutdown  
s2(config-if-range)# exit  
s2(config)# exit
```



Certifique-se de desligar **todas** as portas conectadas para evitar problemas de conexão de rede. Consulte o artigo da Base de Conhecimento. ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) Para obter mais detalhes.

3. Caso ainda não o tenha feito, 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 versões posteriores, use o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, utilize uma ferramenta de comparação ou de diferenças de terceiros.
4. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte:

- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

```
s2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
s2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
s2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
s2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
s2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

Consulte o artigo da Base de Conhecimento ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) Para obter mais detalhes.

5. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

6. Emita o `write erase` comando para apagar a configuração salva atual:

```
s2# 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 para a configuração de inicialização.

```
s2# copy bootflash:write_erase.cfg startup-config
```

8. Reinicie o switch:

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

9. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

10. Copie o RCF para a bootflash do switch s2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Documentação do Cisco Nexus 3000 Series NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um RCF para a bootflash no switch s2:

```
s2# copy tftp: bootflash: vrf management
Enter source filename: NX3232C-RCF-v1.13-1-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)...
```

11. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Documentação da série Cisco Nexus 3000"](#).

Este exemplo mostra o arquivo RCF NX3232C-RCF-v1.13-1-Storage.txt sendo instalado no switch s2:

```
s2# copy NX3232C-RCF-v1.13-1-Storage.txt running-config echo-commands
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

12. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e

consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

13. Reaplique quaisquer personalizações anteriores à configuração do switch.
14. Após verificar se as versões do RCF, as adições personalizadas e as configurações do switch estão corretas, copie o `running-config` arquivo para o `startup-config` arquivo.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Documentação da série Cisco Nexus 9000"](#).

```
s2# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

15. Reinicialize o switch s2. Você pode ignorar os alertas do "monitor de integridade do switch do cluster" e os eventos de "portas do cluster inativas" relatados nos nós enquanto o switch reinicializa.

```
s2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

16. Verifique o status administrativo ou operacional de cada porta de storage do nó e de cada porta de storage shelf.
 - a. Verifique se todas as portas de armazenamento estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status
-----	----	-----	-----	-----	-----	-----
cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- b. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

c. Verifique se os switches estão sendo monitorados:

```
system switch ethernet show
```


Mostrar exemplo

```
cluster1::*> system switch ethernet show
Switch          Type          Address          Model
-----
s1              storage-network  1.2.3.4          N3K-C3232C
  Serial Number: FFFXXXXXXX1
    Is Monitored: true
      Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  10.3(4a)
  Version Source: CDP/ISDP
s2              storage-network  2.3.4.5          N3K-C3232C
  Serial Number: FEEXXXXXXX2
    Is Monitored: true
      Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  10.3(4a)
  Version Source: CDP/ISDP
```

17. Repita as etapas de 1 a 16 no switch s1.

Etapa 3: verifique a rede de storage

Conclua as seguintes etapas em cada switch de storage para verificar se a rede de storage está funcionando corretamente após a atualização do RCF.

1. Verifique se as portas do switch estão **up**.

```
show interface brief
```

2. Verifique se as portas de storage do nó esperadas ainda estão conectadas:

```
show cdp neighbors
```

3. Verifique se as portas esperadas do compartimento de storage ainda estão conectadas:

```
show lldp neighbors
```

4. Verifique se as portas de storage do nó e as portas do shelf de storage estão nas VLANs corretas usando

os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

O que vem a seguir?

Após atualizar seu RCF, você pode ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches.

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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIAbm1zdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer           1          enabled
(switch)#
```



Ao habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Ver ["Configure a segurança de rede usando FIPS."](#) Para obter mais detalhes.

O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar monitoramento de integridade do switch"](#).

Redefina o switch de armazenamento 3232C para os padrões de fábrica

Para restaurar as configurações de fábrica do switch de armazenamento 3232C, você deve apagar as configurações do switch de armazenamento 3232C.

Sobre esta tarefa

- Você precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

Passos

1. Apagar a configuração existente:

```
write erase
```

```
(s2) # 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
```

```
(s2) # 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.

O que vem a seguir

Após reiniciar o interruptor, você pode ["reconfigurar"](#) configurá-lo de acordo com suas necessidades.

Substitua um switch de armazenamento Cisco Nexus 3232C

Siga estes passos para substituir um switch de armazenamento Cisco Nexus 3232C defeituoso. Este é um procedimento não disruptivo.

Requisitos de revisão

A configuração de rede existente deve apresentar as seguintes características:

- A página de switches Ethernet da Cisco contém as versões mais recentes do RCF e do NX-OS para seus switches.
- A conectividade de gerenciamento deve existir em ambos os switches.



Certifique-se de que todas as etapas de solução de problemas foram concluídas para confirmar se o seu switch precisa ser substituído.

O switch Cisco Nexus 3232C de substituição deve ter as seguintes características:

- A conectividade da rede de gerenciamento deve estar funcional.
- O acesso ao console do interruptor de substituição deve estar configurado corretamente.
- A imagem apropriada do sistema operacional RCF e NX-OS deve ser carregada no switch.
- A personalização inicial do interruptor deve estar concluída.

Substitua o interruptor

Este procedimento substitui o segundo switch de storage Nexus 3232C s2 pelo novo switch 3232C ns2. Os dois nós são cluster1-01 e cluster1-02.

Passo 1: confirme se o switch a ser substituído é o s2

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Verifique o status de integridade das portas do nó de storage para garantir que há conexão com o switch de storage s1:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
cluster1-01	e5a	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
cluster1-02	e5a	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

3. Verifique se o switch de storage s1 está disponível:

```
network device-discovery show
```

Mostrar exemplo

```
storage::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
           e5a    s1                        Ethernet1/1
NX3232C
           e4a    cluster1-02              e4a
AFF-A700
           e4e    cluster1-02              e4e
AFF-A700
cluster1-01/lldp
           e5a    s1                        Ethernet1/1      -
           e4a    cluster1-02              e4a
-
           e4e    cluster1-02              e4e
-
cluster1-02/cdp
           e3a    s1                        Ethernet1/2
NX3232C
           e4a    cluster1-01              e4a
AFF-A700
           e4e    cluster1-01              e4e
AFF-A700
cluster1-02/lldp
           e3a    s1                        Ethernet1/2      -
           e4a    cluster1-01              e4a
-
           e4e    cluster1-01              e4e
-
.
.
```

4. Execute o `show lldp neighbors` Execute o comando no switch em funcionamento para confirmar que você consegue visualizar ambos os nós e todas as prateleiras:

```
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
cluster1-01              Eth1/1             121        S           e5a
cluster1-02              Eth1/2             121        S           e5a
SHFGD2008000011          Eth1/5             121        S           e0a
SHFGD2008000011          Eth1/6             120        S           e0a
SHFGD2008000022          Eth1/7             120        S           e0a
SHFGD2008000022          Eth1/8             120        S           e0a
```

Etapa 2: Configurar a cablagem

1. Verifique as portas das prateleiras no sistema de armazenamento:

```
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   -            -
```

2. Remova todos os cabos conectados ao switch de storage s2.
3. Reconecte todos os cabos ao switch de substituição ns2.

Etapa 3: verifique todas as configurações do dispositivo no switch ns2

1. Verifique o estado de integridade das portas do nó de armazenamento:

storage port show -port-type ENET

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						

cluster1-01						
30	e5a	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
cluster1-02						
30	e5a	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						
.						
.						

2. Verifique se ambos os interruptores estão disponíveis:

network device-discovery show

Mostrar exemplo

```
storage::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
           e5a    s1                        Ethernet1/1
NX3232C
           e4a    cluster1-02              e4a          AFF-
A700
           e4e    cluster1-02              e4e          AFF-
A700
           e7b    ns2                      Ethernet1/1
NX3232C
cluster1-01/lldp
           e5a    s1                        Ethernet1/1    -
           e4a    cluster1-02              e4a          -
           e4e    cluster1-02              e4e          -
           e7b    ns2                      Ethernet1/1    -
cluster1-02/cdp
           e5a    s1                        Ethernet1/2
NX3232C
           e4a    cluster1-01              e4a          AFF-
A700
           e4e    cluster1-01              e4e          AFF-
A700
           e7b    ns2                      Ethernet1/2
NX3232C
cluster1-02/lldp
           e5a    s1                        Ethernet1/2    -
           e4a    cluster1-01              e4a          -
           e4e    cluster1-01              e4e          -
           e7b    ns2                      Ethernet1/2    -
.
.
```

3. Verifique as portas das prateleiras no sistema de armazenamento:

```
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  
.  
.
```

4. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir o interruptor, você pode ["configurar monitoramento de integridade do switch"](#).

Atualizar um switch de armazenamento Cisco Nexus 3232C

Siga estes passos para atualizar o software Cisco NX-OS e os arquivos de configuração de referência (RCF) nos switches Cisco Nexus 3232C.

Requisitos de revisão

Antes de começar

Certifique-se de que as seguintes condições sejam atendidas antes de atualizar o software NX-OS e os RCFs no switch de armazenamento:

- O switch está funcionando perfeitamente (não deve haver erros nos registros ou problemas semelhantes).
- Você verificou ou configurou as variáveis de inicialização desejadas no RCF para refletir as imagens de inicialização desejadas, caso esteja instalando apenas o NX-OS e mantendo sua versão atual do RCF.

Se precisar alterar as variáveis 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 reinicializações futuras.

- Você consultou os guias de software e atualização apropriados disponíveis na ["Switches Cisco Nexus série 3000"](#) página para obter a documentação completa sobre os procedimentos de upgrade e downgrade do armazenamento Cisco.
- O número de portas 10 GbE e 40/100 GbE é definido nos arquivos de configuração de referência (RCFs) disponíveis na ["Switches Ethernet Cisco®"](#) página.

Substitua o interruptor

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois storage switches são s1 e s2.
- Os nós são cluster1-01 e cluster1-02.

Os exemplos neste procedimento utilizam dois nós; cluster1-01 com duas portas de armazenamento e cluster1-02 com duas portas de armazenamento. Consulte o "[Hardware Universe](#)" para verificar as portas de armazenamento corretas em suas plataformas. Consulte "[Que informações adicionais preciso para instalar meu equipamento que não está no HWU?](#)" para obter mais informações sobre os requisitos de instalação do switch.



O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma. Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Passo 1: Verifique o estado de funcionamento dos switches e portas.

1. Se o AutoSupport estiver ativado, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Verifique se os switches de armazenamento estão disponíveis:

```
system switch ethernet show
```

Mostrar exemplo

```
storage::*> system switch ethernet show
```

Switch	Type	Address	Model

s1	storage-network	172.17.227.5	NX3232C
Serial Number: FOC221206C2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(3)			
Version Source: CDP			
s2	storage-network	172.17.227.6	NX3232C
Serial Number: FOC220443LZ			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(3)			
Version Source: CDP			

2 entries were displayed.
storage::*>

3. 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
```

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						

cluster1-01						
30	e5a	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
cluster1-02						
30	e5a	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
.						
.						

4. Verifique se não há problemas com o switch de armazenamento ou com a fiação:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance
```

There are no entries matching your query.

Etapa 2: Copie o RCF para o switch Cisco s2

1. Copie o RCF no switch s2 para a memória flash de inicialização do switch usando um dos seguintes protocolos de transferência: FTP, HTTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Mostrar exemplo

O exemplo a seguir mostra o uso do HTTP para copiar um RCF para a bootflash no switch s2:

```
s2# copy http://172.16.10.1//cfg/Nexus_3232C_RCF_v1.6-Storage.txt
bootflash: vrf management
% Total      % Received % Xferd  Average   Speed  Time     Time
Time                               Current          Dload    Upload  Total   Spent
Left                               Speed
 100          3254      100    3254      0        0      8175      0
--:--:-- --:--:-- --:--:--    8301
Copy complete, now saving to disk (please wait)...
Copy complete.
s2#
```

2. Aplique o RCF previamente baixado à memória flash de inicialização:

```
copy bootflash:
```

Mostrar exemplo

O exemplo a seguir mostra o arquivo RCF Nexus_3232C_RCF_v1.6-Storage.txt sendo instalado no switch s2:

```
s2# copy Nexus_3232C_RCF_v1.6-Storage.txt running-config echo-
commands
```

3. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.



Na saída do banner do `show banner motd` Para executar o comando, você deve ler e seguir as instruções na seção **NOTAS IMPORTANTES** para garantir a configuração e o funcionamento corretos do switch.

+

.Mostrar exemplo


```
s2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3232C
* Filename  : Nexus_3232C_RCF_v1.6-Storage.txt
* Date      : Oct-20-2020
* Version   : v1.6
*
* Port Usage : Storage configuration
* Ports 1-32: Controller and Shelf Storage Ports
* Ports 33-34: Disabled
*
* IMPORTANT NOTES*
* - This RCF utilizes QoS and requires TCAM re-configuration,
  requiring RCF
*   to be loaded twice with the Storage 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
*****
*****
s2#
```



Ao aplicar o RCF pela primeira vez, a mensagem **ERRO: Falha ao gravar comandos VSH** é esperada e pode ser ignorada.

4. Após verificar se as versões do software e as configurações do switch estão corretas, copie o arquivo `running-config` para o arquivo `startup-config` no switch `s2`.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em "[Referências de comandos do Cisco Nexus série 3000 NX-OS](#)".

Mostrar exemplo

O exemplo a seguir mostra o `running-config` O arquivo foi copiado com sucesso para o `startup-config` arquivo:

```
s2# copy running-config startup-config
[#####] 100% Copy complete.
```

Etapa 3: copie a imagem do NX-OS para o switch Cisco s2 e reinicialize

1. Copie a imagem do NX-OS para o switch `s2`.

Mostrar exemplo

```
s2# 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.

s2# 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.
```

2. Instale a imagem do sistema para que a nova versão seja carregada na próxima vez que o switch S2 for reiniciado.

O switch será reiniciado em 10 segundos com a nova imagem, conforme mostrado na saída a seguir:

Mostrar exemplo

```
s2# 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):v08.23(09/23/2015)
v08.38(05/29/2020)      no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y
input string too long
```

```
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.
s2#
```

3. Salve a configuração.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Você será solicitado a reiniciar o sistema.

Mostrar exemplo

```
s2# copy running-config startup-config
[] 100% Copy complete.
s2# reload
This command will reboot the system. (y/n)? [n] y
```

4. Confirme se o novo número da versão do NX-OS está no switch:

Mostrar exemplo

```
s2# 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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: S2
  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 due to upgrade
System version: 9.3(3)
Service:
```

```
plugin
  Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
s2#
```

Etapa 4: Verifique novamente o estado de funcionamento dos switches e portas.

1. Verifique novamente se os switches de armazenamento estão disponíveis após a reinicialização:

```
system switch ethernet show
```

Mostrar exemplo

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
s1
                                     storage-network      172.17.227.5
NX3232C
  Serial Number: FOC221206C2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(4)
  Version Source: CDP

s2
                                     storage-network      172.17.227.6
NX3232C
  Serial Number: FOC220443LZ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(4)
  Version Source: CDP
```

2. Verifique se as portas do switch estão funcionando corretamente e operacionais após a reinicialização:

```
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
-----
----
cluster1-01
30            e5a  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
cluster1-02
30            e5a  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
```

3. Verifique novamente se não há problemas com os switches de armazenamento ou com a fiação do cluster:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

4. Repita o procedimento para atualizar o software NX-OS e o RCF no switch s1.
5. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Após atualizar seu switch, você pode ["configurar monitoramento de integridade do switch"](#).

NVIDIA SN2100

Começar

Fluxo de trabalho de instalação e configuração para switches NVIDIA SN2100

O NVIDIA SN2100 é um switch Ethernet que permite a troca de dados entre controladores e gabinetes de discos.

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 instalação e manutenção do switch NVIDIA SN2100, certifique-se de revisar todos os requisitos.

Requisitos de instalação

Se você deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar interruptores de gerenciamento adicionais, que são opcionais.

Você instala o switch NVIDIA SN2100 (X190006/X190106) no gabinete de switch duplo/simples da NVIDIA com os suportes padrão que acompanham o switch.

Para diretrizes de cabeamento, consulte ["Considerações sobre cabeamento e configuração"](#).

Suporte para ONTAP e Linux

O switch NVIDIA SN2100 é um switch Ethernet de 10/25/40/100 Gb que executa o sistema operacional Cumulus Linux. O switch suporta o seguinte:

- ONTAP 9.10.1P3. O switch SN2100 serve aplicações de Cluster e Armazenamento no ONTAP 9.10.1P3 em diferentes pares de switches. A partir do ONTAP 9.10.1P3, você pode usar switches NVIDIA SN2100 para combinar funcionalidades de armazenamento e cluster em uma configuração de switch compartilhada.
- Cumulus Linux (CL) OS versão 4.4.3. Para informações atuais de compatibilidade, consulte ["Switches Ethernet NVIDIA"](#).
- Você pode instalar o Cumulus Linux quando o switch estiver executando o Cumulus Linux ou o ONIE.

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

Componentes e números de peça para switches NVIDIA SN2100

Para a instalação e manutenção do switch NVIDIA SN2100, certifique-se de consultar a lista de componentes e os números de peça do gabinete e do kit de trilhos.

Detalhes do gabinete

Você instala o switch NVIDIA SN2100 (X190006/X190106) no gabinete de switch duplo/simples da NVIDIA com os suportes padrão que acompanham o switch.

Detalhes do kit de trilhos

A tabela a seguir lista o número da peça e a descrição dos interruptores e kits de trilhos MSN2100:

Número da peça	Descrição
X190006-PE	Cluster Switch, NVIDIA SN2100, 16PT 100G, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16PT 100G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16PT 100G, PTSX, Front End
X190106-FE-PI	Switch, NVIDIA SN2100, 16PT 100G, PSIN, Front End
X-MTEF-KIT-D	Kit de trilhos, interruptor duplo NVIDIA lado a lado
X-MTEF-KIT-E	Kit de trilhos, NVIDIA Single Switch de profundidade reduzida



Consulte a documentação da NVIDIA para obter detalhes sobre ["Instalando seu kit de trilhos e interruptor SN2100"](#).

O que vem a seguir

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches NVIDIA SN2100

Para a instalação 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
"Configure e configure seus switches NVIDIA SN2100"	Este manual descreve como configurar e instalar seus switches NVIDIA SN2100, incluindo a instalação do Cumulus Linux e dos RCFs aplicáveis.
"Migre de um switch de armazenamento Cisco para um switch de armazenamento NVIDIA SN2100."	Descreve como migrar de ambientes que usam switches de armazenamento Cisco para ambientes que usam switches de armazenamento NVIDIA SN2100.
"Migre para um cluster comutado de dois nós"	Descreve como migrar para um ambiente comutado de dois nós usando switches NVIDIA SN2100.
"Substitua um switch de armazenamento NVIDIA SN2100"	Descreve o procedimento para substituir um switch de armazenamento NVIDIA SN2100 defeituoso e para fazer o download do Cumulus Linux e do arquivo de configuração de referência.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Permite confirmar o hardware compatível, como switches de armazenamento e cabos, para o modelo da sua plataforma.

Instalar 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."

Analise os requisitos para conexões ópticas, o adaptador QSA e a velocidade da porta do switch.

3

"Conecte os cabos às prateleiras NS224."

Siga os procedimentos de cabeamento se você tiver um sistema no qual os gabinetes de unidades NS224 precisam ser cabeados como armazenamento conectado ao switch (e não como armazenamento conectado diretamente).

Instale o hardware para o switch NVIDIA SN2100.

A instalação do hardware do switch NVIDIA SN2100 é um primeiro passo crucial na construção de uma infraestrutura de rede confiável e escalável para suportar fluxos de trabalho de proteção, replicação e gerenciamento de dados.

Siga estas etapas para configurar seus switches SN2100. Consulte a documentação da NVIDIA para obter instruções detalhadas.

Passos

- 1. Analise o ["requisitos de configuração"](#) .
- 2. Siga as instruções no ["Guia de Instalação do NVIDIA Switch"](#).

O que vem a seguir?

Após instalar o hardware, você pode ["revisar cabeamento e configuração"](#) requisitos.

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seu switch NVIDIA SN2100, revise as seguintes considerações.

Detalhes da porta NVIDIA

Portas de comutação	Utilização de portas
swp1s0-3	Nós de porta de cluster breakout 4x10GbE
swp2s0-3	Nós de porta de cluster breakout 4x25GbE
swp3-14	nós de porta de cluster 40/100GbE

Consulte o "[Hardware Universe](#)" para obter mais informações sobre portas de switch.

Atrasos na conexão com ligações ópticas

Se você estiver enfrentando atrasos na conexão superiores a cinco segundos, o Cumulus Linux 5.4 e versões posteriores incluem suporte para conexão rápida. Você pode configurar os links usando o `nv set`. O comando é o seguinte:

```
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 seguintes ao `/etc/cumulus/switchd.conf` Arquivo para cada porta (swp<n>) que utiliza 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 o `switchd` 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` O comando é o seguinte:

- ° `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 Knowledge Base ["O switch SN2100 não consegue se conectar 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 placas de rede X1151A, placas de rede X1146A ou portas 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 conectar-se às portas de cluster 10GbE/25GbE em uma plataforma, a conexão pode não ser estabelecida.

Para resolver esse problema, faça o seguinte:

- Para 10GbE, defina manualmente a velocidade de link do swp1s0-3 para 10000 e desative a negociação automática.
- Para 25GbE, defina manualmente a velocidade de link do swp2s0-3 para 25000 e desative a negociação automática.



Ao usar adaptadores QSA de 10GbE/25GbE, insira-os em portas 40GbE/100GbE que não sejam de breakout (swp3-swp14). Não insira o adaptador QSA em uma porta configurada para breakout.

Defina a velocidade da interface nas portas de breakout.

Dependendo do transceptor na porta do switch, pode ser necessário definir a velocidade na interface do switch para uma velocidade fixa. Se estiver usando portas breakout de 10GbE e 25GbE, verifique se a negociação automática está desativada e configure 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 o status da interface e da porta para confirmar se as configurações foram 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 o status da interface e da porta para confirmar se as configurações foram 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 vem a seguir?

Após analisar os requisitos de cabeamento e configuração, você pode ["Conecte os racks NS224 como armazenamento conectado por switch."](#) .

Prateleiras Cable NS224 como armazenamento conectado ao switch

Se você possui um sistema no qual os gabinetes de unidades NS224 precisam ser cabeados como armazenamento conectado por switch (e não como armazenamento conectado diretamente), utilize as informações fornecidas aqui.

- O cabo NS224 aciona as prateleiras através dos switches de armazenamento:

["Informações para cabeamento de gavetas de unidades NS224 conectadas a switches"](#)

- Instale seus switches de armazenamento:

["Documentação dos interruptores AFF e FAS"](#)

- Confirme o hardware compatível, como switches de armazenamento e cabos, para o modelo da sua plataforma. Consulte a ["Hardware Universe"](#) para obter detalhes.

Configurar software

Fluxograma de instalação de software para switches de armazenamento NVIDIA SN2100

Para instalar e configurar o software de um switch NVIDIA SN2100, siga estes passos:

1

["Configure o interruptor"](#)

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 do Arquivo de Configuração de Referência \(RCF\)"](#)

Existem dois scripts RCF disponíveis para aplicações de Clustering e Armazenamento. O procedimento é o mesmo para todos.

5

["Instale o arquivo CSHM"](#)

Você pode instalar o arquivo de configuração aplicável para o monitoramento da integridade dos switches Ethernet em clusters NVIDIA .

Configure o switch NVIDIA SN2100

Para configurar o switch SN2100, consulte a documentação da NVIDIA.

Passos

1. Analise o ["requisitos de configuração"](#) .
2. Siga as instruções em ["Inicialização do sistema NVIDIA ."](#) .

O que vem a seguir?

Depois de configurar seus switches, você pode ["Instale o Cumulus Linux no modo Cumulus."](#) ou ["Instalar o Cumulus Linux no modo ONIE"](#) .

Instale o Cumulus Linux no modo Cumulus.

Siga este procedimento para instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver em modo Cumulus.



O sistema operacional Cumulus Linux (CL) pode ser instalado quando o switch está executando Cumulus Linux ou ONIE (consulte ["Instalar no modo ONIE"](#)).

Antes de começar

Certifique-se de que o seguinte esteja disponível:

- Conhecimento intermediário de Linux.
- Familiaridade com edição básica de texto, permissões de arquivos UNIX e monitoramento de processos. Diversos editores de texto vêm pré-instalados, incluindo: `vi` e `nano` .
- Acesso a um shell Linux ou UNIX. Se você estiver usando o Windows, utilize um ambiente Linux como ferramenta de linha de comando para interagir com o Cumulus Linux.
- A taxa de transmissão (baud rate) deve ser configurada para 115200 no switch de console serial para acesso ao console do switch NVIDIA SN2100, conforme descrito a seguir:
 - 115200 baud
 - 8 bits de dados
 - 1 bit de parada
 - paridade: nenhuma
 - Controle de fluxo: nenhum

Sobre esta tarefa

Esteja ciente do 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 cumulus é **cumulus**. Na primeira vez que você fizer login no Cumulus Linux, você deverá alterar esta senha padrão. Certifique-se de atualizar todos os scripts de automação antes de instalar uma nova imagem. O Cumulus Linux oferece 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. Faça login no switch.

O primeiro acesso ao switch requer o nome de usuário/senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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. Atualização para o novo fuso horário:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

- c. Verifique seu 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. Configure 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 valor do 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 utiliza 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 o download. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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-o ao `sudo` grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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. Faça login no switch.

O primeiro acesso ao switch requer o nome de usuário/senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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 seu 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. Configure 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 valor do 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
```

Consulte o artigo da Knowledge Base ["A configuração do servidor NTP não está funcionando com switches NVIDIA SN2100."](#) para obter 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 utiliza 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 o download. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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 cada nó possui 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-o ao `sudo` grupo. Este usuário só entra em vigor após a reinicialização da sessão de console/SSH.

```
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 o usuário administrador acessar. **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 NVIDIA](#)" para mais informações.

Cumulus Linux 5.11.0

1. Faça login no switch.

Ao fazer login no switch pela primeira vez, é necessário inserir o nome de usuário e a senha **cumulus/cumulus**. sudo privilégios.

```
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 do 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 entra em vigor após reiniciar o console/sessão SSH.



Um switch Cumulus Linux fornece pelo menos uma porta Ethernet dedicada para gerenciamento, chamada `eth0`. Esta interface destina-se especificamente à gestão fora de banda. Por padrão, a interface de gerenciamento usa DHCPv4 para endereçamento.



Não utilize sublinhado (`_`), apóstrofo (`'`) ou caracteres 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 ambos os `/etc/hostname` e `/etc/hosts` arquivos.

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. Configure 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 seu 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. Configure 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 valor do 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
```

Consulte o artigo da Knowledge Base ["A configuração do servidor NTP não está funcionando com switches NVIDIA SN2100."](#) para obter 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 utiliza 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 o download. Digite **y** quando solicitado.

7. Reinicie o switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. A instalação inicia automaticamente e as seguintes opções da tela GRUB são exibidas. Não faça nenhuma seleção.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar SO
- CUMULUS-INSTALAÇÃO
- Cumulus-Linux GNU/Linux

9. Repita os passos de 1 a 4 para fazer login.

10. Verifique se a versão do 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 possui 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 NVIDIA"](#) para mais informações.

O que vem a seguir?

Após instalar o Cumulus Linux no modo Cumulus, você pode ["Instalar ou atualizar o script RCF"](#).

Instale o Cumulus Linux no modo ONIE.

Siga este procedimento para instalar o sistema operacional Cumulus Linux (CL) quando o switch estiver em modo ONIE.



O sistema operacional Cumulus Linux (CL) pode ser instalado quando o switch está executando Cumulus Linux ou ONIE (consulte ["Instalar no modo Cumulus"](#)).

Sobre esta tarefa

Você pode instalar o Cumulus Linux usando o Open Network Install Environment (ONIE), que permite a descoberta automática de uma imagem de instalação de rede. Isso facilita o modelo de sistema para proteger switches com uma opção de sistema operacional, como o Cumulus Linux. A maneira mais fácil de instalar o Cumulus Linux com ONIE é através da descoberta HTTP local.



Se o seu host estiver habilitado para IPv6, certifique-se de que ele esteja executando um servidor web. Se o seu host estiver habilitado para IPv4, certifique-se de que ele esteja executando o DHCP além de um servidor web.

Este procedimento demonstra como atualizar o Cumulus Linux depois que o administrador inicializou o sistema no ONIE.

Passos

1. Faça o download do arquivo de instalação do Cumulus Linux para o diretório raiz do servidor web. Renomeie este arquivo `onie-installer`.
2. Conecte seu computador à porta Ethernet de gerenciamento do switch usando um cabo Ethernet.
3. Ligue o interruptor. O switch baixa o instalador de imagem ONIE e inicializa. Após a conclusão da instalação, a tela 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. Na tela do GNU GRUB, pressione a tecla **Esc** para interromper o processo normal de inicialização, selecione **ONIE** e pressione **Enter**.
6. Na próxima tela exibida, selecione **ONIE: Instalar SO**.
7. O processo de descoberta do instalador ONIE é executado em busca da instalação automática. Pressione **Enter** para interromper temporariamente o processo.
8. Quando o processo de descoberta for concluído:

```
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 sua rede, verifique se o endereço IP, a máscara de sub-rede e o gateway padrão estão atribuídos corretamente:

```
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 inseridas corretamente.

12. Instalar 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. Após a conclusão da instalação, faça login no switch:

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 do 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 vem a seguir?

Após instalar o Cumulus Linux no modo ONIE, você pode "[Instalar ou atualizar 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 os seguintes itens estejam disponíveis no switch:

- O Cumulus Linux 4.4.3 está instalado.
- Endereço IP, máscara de sub-rede e gateway padrão definidos via DHCP ou configurados manualmente.

Versões atuais do script RCF

Existem dois scripts RCF disponíveis para aplicações de Clustering e Armazenamento. O procedimento é o mesmo para todos.

- Agrupamento: **MSN2100-RCF-v1.x-Cluster**
- Armazenamento: **MSN2100-RCF-v1.x-Armazenamento**



O procedimento de exemplo a seguir mostra como baixar e aplicar o script RCF para switches de cluster.



O comando de exemplo utiliza o endereço IP de gerenciamento do switch 10.233.204.71, máscara de rede 255.255.254.0 e gateway padrão 10.233.204.1.

Passos

1. Exibir as interfaces disponíveis no switch 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 com o script Python do RCF que não possam ser corrigidos, entre em contato com "[Suporte NetApp](#)" para obter assistência.

4. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração.](#)" 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 transceptor 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 cada nó possui 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 do 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 o estado de saúde do switch no cluster (o switch sw2 pode não ser exibido, pois as LIFs não estão configuradas 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 vem a seguir?

Após instalar ou atualizar o RCF, você pode [Instale o arquivo CSHM](#) .

Instale o arquivo de configuração do Monitor de Saúde do Switch Ethernet.

Siga este procedimento para instalar o arquivo de configuração aplicável para monitoramento da integridade do switch Ethernet em switches de 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 versões posteriores.

Antes de começar

- Verifique se você precisa baixar o arquivo de configuração executando o seguinte comando: `system switch ethernet show` e verificando se **OUTRO** é exibido para o seu modelo.

Se o seu modelo ainda estiver exibindo **OUTRO** após a aplicação do arquivo de configuração, entre em contato com o suporte da NetApp .

- Certifique-se de que o cluster ONTAP esteja ativo e em funcionamento.
- Habilite 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 shell do nó:

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

- b. Alteração para privilégios avançados:

```
priv set advanced
```

- c. Liste os arquivos de configuração em `/etc/cshm_nod/nod_sign` diretório. Se o diretório existir e contiver arquivos de configuração, ele listará os nomes dos arquivos.

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

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

Caso não tenha certeza, remova todos os arquivos de configuração dos modelos compatíveis listados acima e, em seguida, baixe e instale os arquivos 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. Baixe o arquivo zip de configuração do monitor de integridade do switch Ethernet, de acordo com a versão do ONTAP correspondente. Este arquivo está disponível em "[Switches Ethernet NVIDIA](#)" página.
 - a. Na página de download do software NVIDIA SN2100, selecione **Arquivo CSHM da NVIDIA**.
 - b. Na página de Atenção/Leitura Obrigatória, selecione a caixa de seleção para concordar.
 - c. Na página do Contrato de Licença do Usuário Final, selecione a caixa de seleção para concordar e clique em **Aceitar e Continuar**.
 - d. Na página de download do arquivo CSHM da Nvidia, selecione o arquivo de configuração aplicável. Os seguintes arquivos estão disponíveis:

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 a 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. [[passo 2]]Faça o upload do arquivo zip correspondente para o seu servidor web interno.
2. Acesse as configurações do modo avançado a partir de um dos sistemas ONTAP no cluster.

```
set -privilege advanced
```

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

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

4. Verifique se a saída do comando termina com o seguinte texto para a 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 a 9.14.1

O SHM instalou o arquivo de configuração.

ONTAP 9.10.1

O pacote CSHM foi baixado e processado com sucesso.

Caso ocorra algum erro, entre em contato com o suporte da NetApp .

1. [[passo 6]]Aguarde até o dobro do intervalo de sondagem do monitor de integridade do switch Ethernet, determinado executando `system switch ethernet polling-interval show` , antes de concluir a próxima etapa.
2. Execute o comando `system switch ethernet configure-health-monitor show` No sistema ONTAP , certifique-se de que os switches do cluster sejam descobertos com o campo monitorado definido como **Verdadeiro** e o campo do número de série não mostrando **Desconhecido**.

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

O que vem a seguir?

Após instalar o arquivo CSHM, você pode ["configurar 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 o Cumulus Linux 5.11 e versões posteriores, você usa o `nv action reset system factory-default` comando.

Sobre esta tarefa

- Você precisa estar conectado 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. A partir do console do Cumulus, baixe e coloque na fila a instalação do software do switch com o comando `onie-install -a -i` seguido do caminho do arquivo do software de comutação, 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 reinicia e permanece no estado em que foi instalado. `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
```

Consulte a documentação da NVIDIA "[Redefinição de fábrica](#)" para obter mais detalhes.

O que vem a seguir

Depois de reiniciar os interruptores, você pode "[reconfigurar](#)" eles conforme necessário.

Migrar switches

Migre de um switch de armazenamento Cisco para um switch de armazenamento NVIDIA SN2100.

Você pode migrar switches Cisco mais antigos de um cluster ONTAP para switches de armazenamento NVIDIA SN2100. Este é um procedimento não disruptivo.

Requisitos de revisão

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 suas configurações.

Antes de começar

Certifique-se de ter o seguinte:

- O cluster existente está configurado corretamente e funcionando.
- Todas as portas de armazenamento estão em estado ativo para garantir operações sem interrupções.
- Os switches de armazenamento NVIDIA SN2100 estão configurados e operando na versão correta do Cumulus Linux instalada com o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede de armazenamento existente apresenta as seguintes características:
 - Um cluster NetApp redundante e totalmente funcional, utilizando switches Cisco mais antigos.
 - Conectividade de gerenciamento e acesso ao console tanto para os switches Cisco mais antigos quanto para os novos.
 - Todas as LIFs do cluster estão ativas e conectadas às suas portas de origem.
 - As portas ISL foram habilitadas 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 suas configurações.
- Algumas das portas estão configuradas em switches NVIDIA SN2100 para operar em 100 GbE.
- Você planejou, migrou e documentou a conectividade de 100 GbE dos nós para os switches de armazenamento NVIDIA SN2100.

Migre os switches

Sobre os exemplos

Neste procedimento, os switches de armazenamento Cisco Nexus 9336C-FX2 são usados como exemplos de comandos e saídas.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster são *node1_clus1* e *node1_clus2* no nó 1, e *node2_clus1* e *node2_clus2* no nó 2, respectivamente.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas de rede utilizadas neste procedimento são *e5a* e *e5b*.
- As portas de breakout têm o formato: *swp1s0-3*. Por exemplo, quatro portas de breakout em *swp1* são *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.
- Primeiro, a chave S2 é substituída pela chave *sw2* e, em seguida, a chave S1 é substituída pela chave *sw1*.
 - Os cabos entre os nós e o switch S2 são então desconectados do switch S2 e reconectados ao switch S2.
 - Os cabos entre os nós e o switch S1 são então desconectados do switch S1 e reconectados ao switch *sw1*.

Etapas 1: Prepare-se para a migração

1. Se o AutoSupport estiver ativado, suprima a criação automática de casos invocando uma mensagem do 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, digitando **y** quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (***>**) é exibida.

3. Determine o status administrativo ou operacional de cada interface de armazenamento:

Cada porta deve exibir "habilitado" para `Status` .

Etapas 2: Configurar cabos e portas

1. Exibir os atributos da porta de rede:

```
storage port show
```

Mostrar exemplo

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN 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 armazenamento em cada nó estão conectadas aos switches de armazenamento existentes da seguinte maneira (da perspectiva 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. Nos switches S1 e S2, certifique-se de que as portas de armazenamento e os switches estejam conectados da seguinte maneira (do ponto de vista 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 Port ID	Local Intf	Holdtime	Capability
node1 e0c	Eth1/1	121	S
node2 e0c	Eth1/2	121	S
SHFGD1947000186 e0a	Eth1/10	120	S
SHFGD1947000186 e0a	Eth1/11	120	S
SHFGB2017000269 e0a	Eth1/12	120	S
SHFGB2017000269 e0a	Eth1/13	120	S

```
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 Port ID	Local Intf	Holdtime	Capability
node1 e5b	Eth1/1	121	S
node2 e5b	Eth1/2	121	S
SHFGD1947000186 e0b	Eth1/10	120	S
SHFGD1947000186 e0b	Eth1/11	120	S
SHFGB2017000269 e0b	Eth1/12	120	S
SHFGB2017000269 e0b	Eth1/13	120	S

4. No switch sw2, desligue as portas conectadas às portas de armazenamento e aos nós dos gabinetes de discos.

Mostrar exemplo

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Mova as portas de armazenamento do controlador e dos gabinetes de discos do switch antigo S2 para o novo switch sw2, usando a cablagem apropriada compatível com o NVIDIA SN2100.
6. No switch sw2, ative as portas conectadas às portas de armazenamento dos nós e aos gabinetes de discos.

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 armazenamento em cada nó estão agora conectadas aos switches da seguinte maneira, da perspectiva dos nós:

```
network device-discovery show -protocol lldp
```

Mostrar exemplo

```
cluster1::~*> network device-discovery show -protocol lldp
```

Node/ Protocol	Local Port	Discovered 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
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN 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 armazenamento do nó 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, desligue as portas conectadas às portas de armazenamento dos nós e aos gabinetes de discos.

Mostrar exemplo

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Mova as portas de armazenamento do controlador e os gabinetes de discos do switch antigo S1 para o novo switch sw1, usando a cablagem apropriada compatível com o NVIDIA SN2100.
12. No switch sw1, ative as portas conectadas às portas de armazenamento dos nós e aos gabinetes de discos.

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 armazenamento em cada nó estão agora conectadas aos switches da seguinte maneira, da perspectiva dos nós:

```
network device-discovery show -protocol lldp
```

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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 exibir "habilitado" para State e habilitado para Status .

Mostrar exemplo

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN 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 armazenamento do nó 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 possuem uma conexão com cada switch:

```
net show lldp
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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 administrador:

```
set -privilege admin
```

5. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode [configurar monitoramento de integridade do switch](#).

Substitua um switch de armazenamento NVIDIA SN2100

Você pode substituir um switch de armazenamento NVIDIA SN2100 defeituoso. Este é um procedimento não disruptivo.

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 é compatível com switches de armazenamento NVIDIA SN2100.
- Você baixou os RCFs aplicáveis.

O ["Hardware Universe"](#) fornece detalhes completos sobre as portas suportadas e suas configurações.

A configuração de rede existente deve apresentar as seguintes características:

- Conclua todas as etapas de solução de problemas para confirmar se você precisa substituir o seu interruptor.
- Garanta que exista conectividade de gerenciamento em ambos os switches.



Certifique-se de que todas as etapas de solução de problemas foram concluídas para confirmar se o seu switch precisa ser substituído.

O switch NVIDIA SN2100 de substituição deve ter as seguintes características:

- A conectividade da rede de gerenciamento está 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 interruptor está concluída.

Resumo do procedimento

Este procedimento substitui o segundo switch de armazenamento NVIDIA SN2100 (sw2) pelo novo switch NVIDIA SN2100 (nsw2). Os dois nós são o nó 1 e o nó 2.

Passos para concluir:

- Confirme se o interruptor a ser substituído é o SW2.
- Desconecte os cabos do interruptor sw2.
- Reconecte os cabos ao switch nsw2.
- Verifique todas as configurações do dispositivo no switch nsw2.

Passos

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

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

x representa a duração da janela de manutenção em horas.

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

```
set -privilege advanced
```

3. Verifique o estado 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
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN 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 a chave 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` Execute o comando no switch em funcionamento para confirmar que você consegue visualizar ambos os nós e todas as prateleiras:

```
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 das prateleiras no sistema de armazenamento:

```
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 conectados à chave de armazenamento sw2.
8. Reconecte todos os cabos ao switch de substituição nsw2.
9. Verifique novamente o estado de integridade das portas do nó de armazenamento:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET  
  
Node      Port Type  Mode   Speed      State   Status   VLAN  
-----  -  
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 interruptores 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 das prateleiras no sistema de armazenamento:

```
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 administrador:

```
set -privilege admin
```

13. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Switches compartilhados

Cisco Nexus 9336C-FX2

Começar

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 compartilhados para cluster e armazenamento.

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 instalação e manutenção do switch Cisco Nexus 9336C-FX2, certifique-se de revisar os requisitos de configuração e de rede.

Suporte ONTAP

A partir do ONTAP 9.9.1, você pode usar switches Cisco Nexus 9336C-FX2 para combinar funcionalidades de armazenamento e cluster em uma configuração de switch compartilhada.

Se você deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede compatíveis.

Requisitos de configuração

Para a configuração, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches.

Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch.

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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.

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter as informações mais recentes.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.
- Para obter mais informações sobre a configuração inicial do seu switch, consulte o seguinte: ["Guia de Instalação e Atualização do Cisco Nexus 9336C-FX2"](#).

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

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 consultar a lista de componentes e números de peça.

A tabela a seguir lista o número da peça e a descrição do switch 9336C-FX2, dos ventiladores e das fontes de alimentação:

Número da 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	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de exaustão lateral
X-NXA-PAC-1100W-PI2	Fonte de alimentação N9K-9336C AC 1100W - Fluxo de ar de entrada pelo lado da porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65 CFM, fluxo de ar de exaustão do lado esquerdo
X-NXA-FAN-65CFM-PI	N9K-9336C 65 CFM, fluxo de ar de admissão pelo lado esquerdo

O que vem a seguir

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2

Para a instalação do switch Cisco Nexus 9336C-FX2, certifique-se de revisar a documentação específica do switch e do controlador para configurar seus switches Cisco 9336C-FX2 e o cluster ONTAP.

Para configurar os switches compartilhados Cisco Nexus 9336C-FX2, consulte ["Suporte para switches Cisco Nexus série 9000"](#).

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 de software para switches Cisco Nexus série 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
"Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000" (escolha o guia para a versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
"Índice principal de referência de comandos do Cisco Nexus série 9000 NX-OS"	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
"Referência de MIBs do Cisco Nexus 9000"	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 9000.
"Referência de mensagens do sistema NX-OS da série Nexus 9000"	Descreve as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
"Notas de versão do NX-OS para a série Cisco Nexus 9000" (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.
"Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000"	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale o switch 9336C-FX2.

3

"Instale o switch em um gabinete NetApp ."

Instale o switch 9336C-FX2 e o painel de passagem em um gabinete NetApp , conforme necessário.

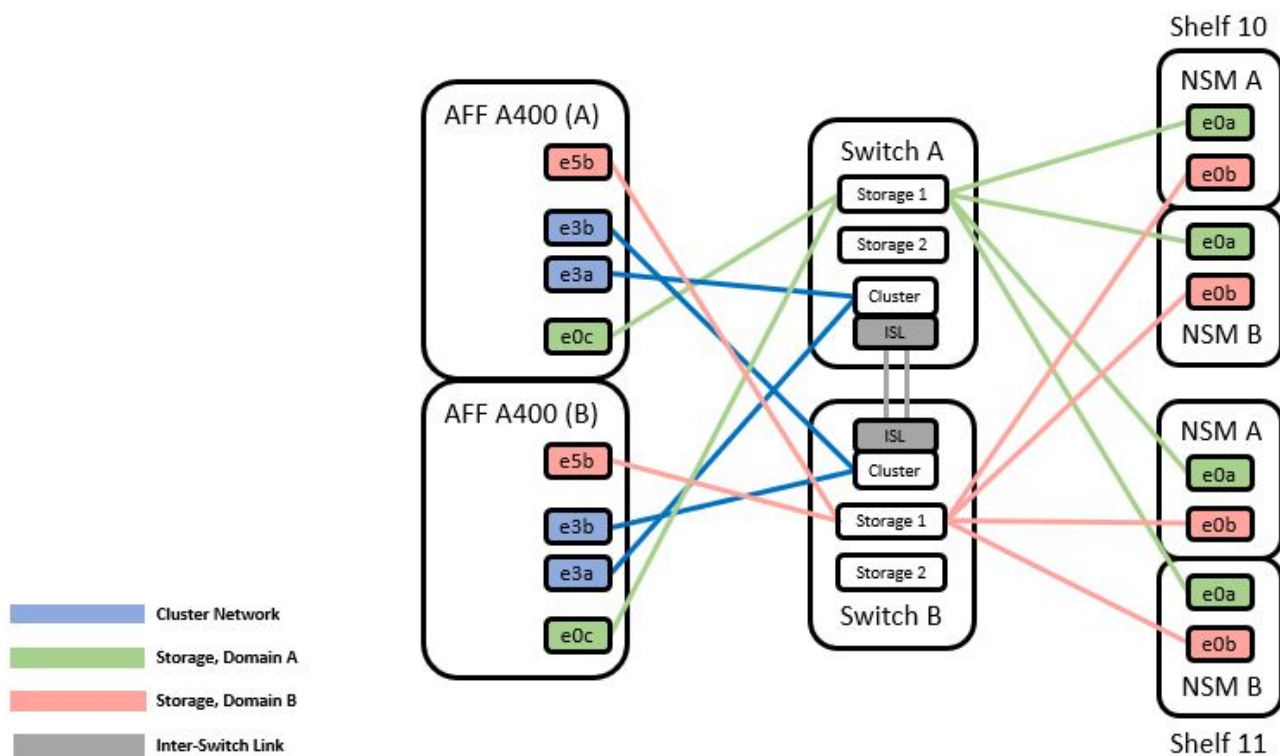
Preencha a planilha de cabeamento do Cisco Nexus 9336C-FX2.

Utilize as imagens de cabeamento a seguir para concluir a conexão entre os controladores e os switches.

Cabo NS224 para armazenamento conectado a um switch

Se você deseja conectar o armazenamento NS224 como um dispositivo conectado a um switch, siga o diagrama de conexão a switch:

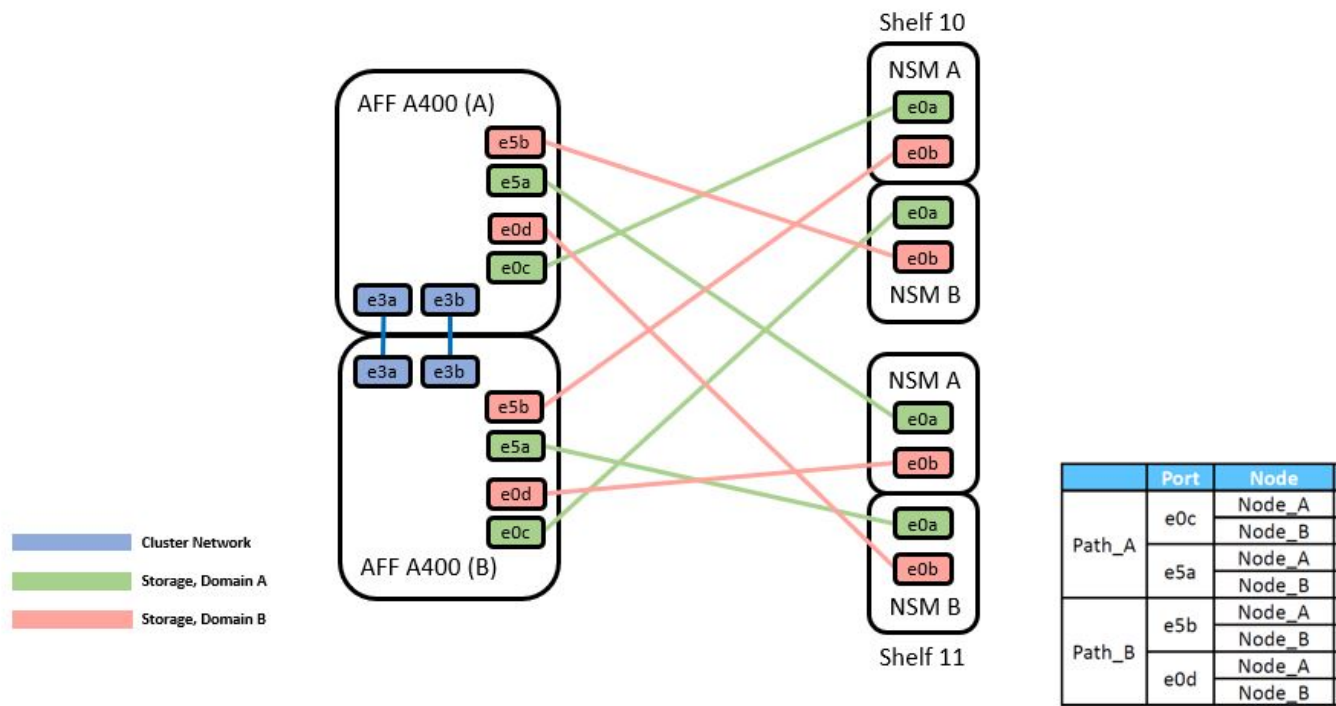
Switch Attached



Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch. Consulte o ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Armazenamento do cabo NS224 como conexão direta

Se você deseja conectar o armazenamento NS224 diretamente em vez de usar as portas de armazenamento compartilhadas do switch, siga o diagrama de conexão direta:



Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.

Folha de instruções de cabeamento do Cisco Nexus 9336C-FX2

Se você deseja documentar as plataformas suportadas, deve preencher a planilha de cabeamento em branco, utilizando como guia a planilha de cabeamento de exemplo já preenchida.

A definição da porta de exemplo 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	40/10GbE	1	Cluster	40/10GbE
2	Cluster	40/10GbE	2	Cluster	40/10GbE
3	Cluster	40/10GbE	3	Cluster	40/10GbE
4	Cluster	40/10GbE	4	Cluster	40/10GbE
5	Cluster	40/10GbE	5	Cluster	40/10GbE
6	Cluster	40/10GbE	6	Cluster	40/10GbE
7	Cluster	40/10GbE	7	Cluster	40/10GbE
8	Cluster	40/10GbE	8	Cluster	40/10GbE
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-1	100GbE	11	Storage-1	100GbE
12	Storage-1	100GbE	12	Storage-1	100GbE
13	Storage-1	100GbE	13	Storage-1	100GbE
14	Storage-1	100GbE	14	Storage-1	100GbE
15	Storage-1	100GbE	15	Storage-1	100GbE
16	Storage-1	100GbE	16	Storage-1	100GbE
17	Storage-1	100GbE	17	Storage-1	100GbE
18	Storage-1	100GbE	18	Storage-1	100GbE
19	Storage-1	100GbE	19	Storage-1	100GbE
20	Storage-1	100GbE	20	Storage-1	100GbE
21	Storage-1	100GbE	21	Storage-1	100GbE
22	Storage-1	100GbE	22	Storage-1	100GbE
23	Storage-2	100GbE	23	Storage-2	100GbE
24	Storage-2	100GbE	24	Storage-2	100GbE
25	Storage-2	100GbE	25	Storage-2	100GbE
26	Storage-2	100GbE	26	Storage-2	100GbE
27	Storage-2	100GbE	27	Storage-2	100GbE
28	Storage-2	100GbE	28	Storage-2	100GbE
29	Storage-2	100GbE	29	Storage-2	100GbE
30	Storage-2	100GbE	30	Storage-2	100GbE
31	Storage-2	100GbE	31	Storage-2	100GbE
32	Storage-2	100GbE	32	Storage-2	100GbE
33	Storage-2	100GbE	33	Storage-2	100GbE
34	Storage-2	100GbE	34	Storage-2	100GbE
35	ISL	100GbE	35	ISL	100GbE
36	ISL	100GbE	36	ISL	100GbE

Onde:

- ISL de 100G para switch A porta 35
- ISL de 100G para switch A porta 36
- ISL de 100G para a porta 35 do switch B
- ISL de 100G para a porta 36 do switch B

Folha de exercícios de cabeamento em branco

Você pode usar a planilha de cabeamento em branco para documentar as plataformas suportadas como nós em um cluster. A tabela Supported Cluster Connections "[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		

Onde:

- ISL de 100G para switch A porta 35

- ISL de 100G para switch A porta 36
- ISL de 100G para a porta 35 do switch B
- ISL de 100G para a porta 36 do switch B

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você pode ["instalar o interruptor"](#).

Instalar switches compartilhados Cisco Nexus 9336C-FX2

Siga estas instruções para configurar os switches compartilhados Cisco Nexus 9336C-FX2.

Antes de começar

Certifique-se de ter o seguinte:

- Documentação necessária do switch compartilhado, documentação do controlador e documentação do ONTAP. Consulte ["Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2"](#) e ["Documentação do NetApp ONTAP"](#).
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Planilhas de cabeamento preenchidas. Consulte ["Preencha a planilha de cabeamento do Cisco Nexus 9336C-FX2"](#). Para mais informações sobre cabeamento, consulte o ["Hardware Universe"](#).

Passos

1. Instale os switches, controladores e gavetas de armazenamento NVMe NS224 no rack.

Consulte ["Instruções de instalação"](#) para saber como instalar o switch em um gabinete NetApp.

2. Ligue os switches, controladores e gavetas de armazenamento NVMe NS224.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 9336C-FX2 em um gabinete NetApp"](#). Caso contrário, acesse ["Configure o interruptor"](#).

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 de passagem em um gabinete NetApp . Suportes padrão estão incluídos com o interruptor.

Antes de começar

Certifique-se de ter o seguinte:

- Para cada interruptor, você deve fornecer os oito parafusos 10-32 ou 12-24 e as porcas de fixação para montar os suportes e os trilhos deslizantes nos postes dianteiro e traseiro do gabinete.
- Você deve usar o kit de trilhos padrão da Cisco para instalar o switch em um gabinete NetApp .



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Documentação necessária

Analise os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança em ["Guia de Instalação de Hardware da Série Cisco Nexus 9000"](#) .

Passos

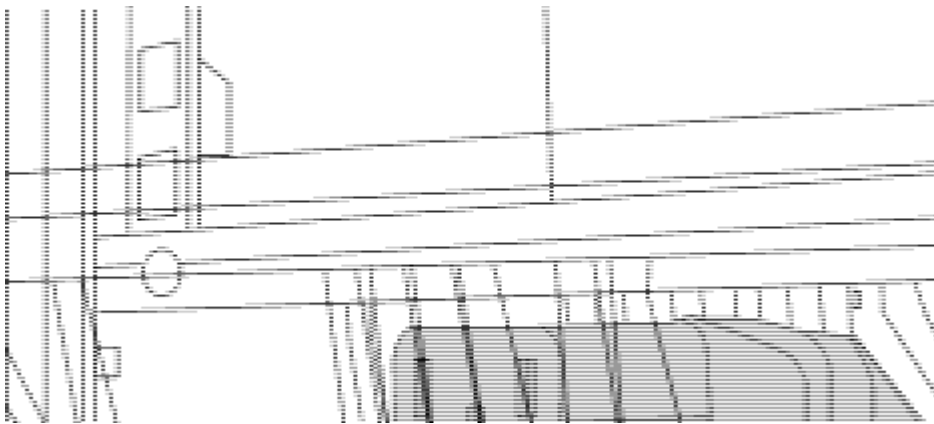
1. Instale o painel de vedação de passagem no gabinete NetApp .

O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

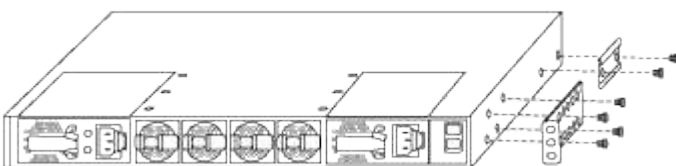
- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
 - i. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - ii. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - iii. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - iv. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.



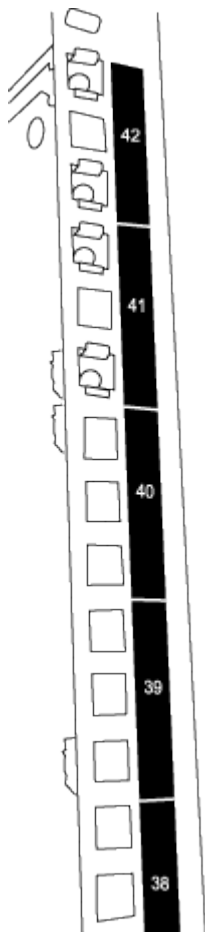
(1) Conector fêmea do cabo jumper.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 9336C-FX2.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.



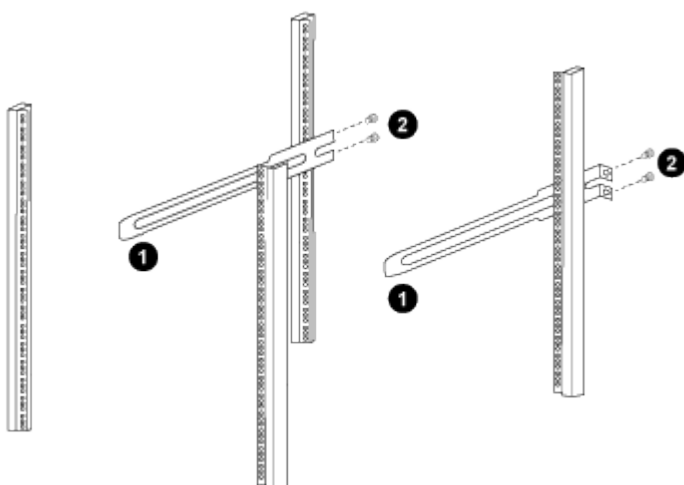
- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.

- c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
3. Instale as porcas de clipe nos locais dos furos quadrados para todos os quatro postes IEA.



Os dois switches 9336C-FX2 sempre serão montados no 2U superior do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no armário.
- a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os com os dedos.



(1) Ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos na cremalheira.

(2) Aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

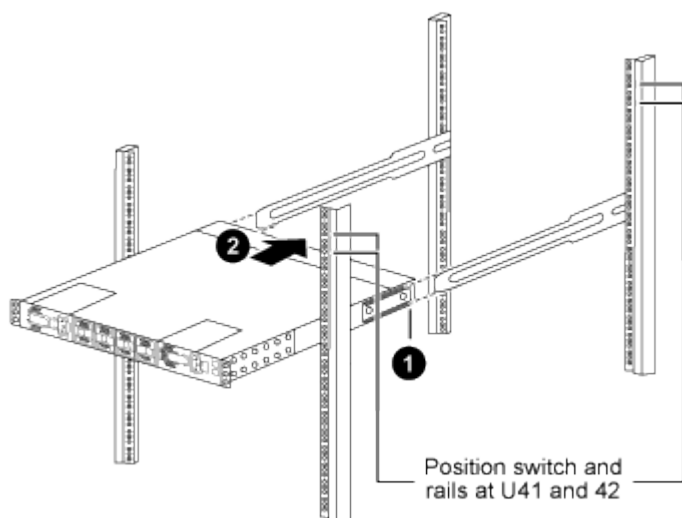
- a. Repita o passo 4a para o poste traseiro do lado direito.
- b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

5. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

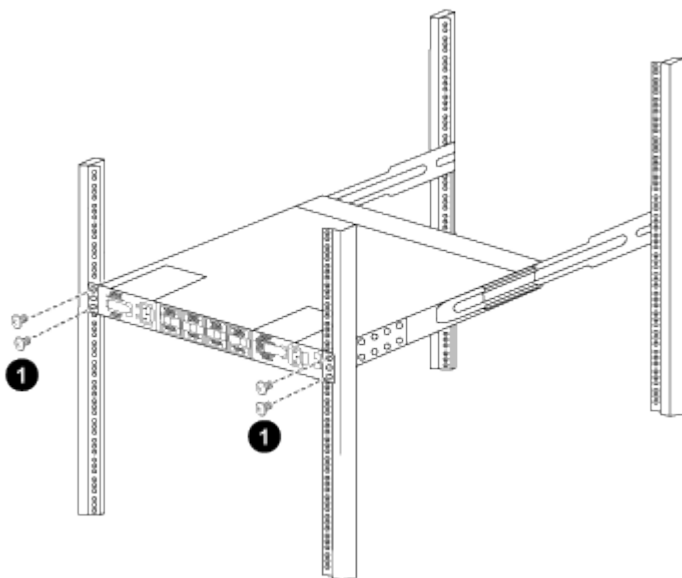
- a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

- b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

- a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos postes.
- b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

6. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
7. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

8. Conecte a porta de gerenciamento em cada switch 9336C-FX2 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seus 9336C-FX2 e 9336C-FX2-T switches, revise os requisitos de cabeamento e configuração.

Suporte para portas Ethernet NVIDIA CX6, CX6-DX e CX7.

Se você estiver conectando uma porta do switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir manualmente 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
```

Requisitos de FEC de 25GbE

Portas FAS2820 e0a/e0b

As portas FAS2820 e0a e e0b requerem alterações na configuração do FEC para se conectarem às portas do switch 9336C-FX2 e 9336C-FX2-T. Para as portas e0a e e0b do switch, a configuração `fec` está 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 conectam 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.

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.
- Consulte o artigo da Knowledge Base ["As portas não se conectam no Cisco Nexus 9336C-FX2 devido a recursos TCAM."](#) para obter detalhes sobre como resolver problemas do TCAM.

Configurar o software

Fluxo de trabalho de instalação de software para switches compartilhados Cisco Nexus 9336C-FX2

Para instalar e configurar o software de um switch compartilhado Cisco Nexus 9336C-FX2, siga estes passos:

1

"Configure o interruptor"

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.

Configurar switches compartilhados Cisco Nexus 9336C-FX2

Siga estas instruções para configurar os switches compartilhados Cisco Nexus 9336C-FX2.

Antes de começar

Certifique-se de ter o seguinte:

- Documentação necessária do switch compartilhado, documentação do controlador e documentação do ONTAP. Consulte "[Requisitos de documentação para switches compartilhados Cisco Nexus 9336C-FX2](#)" e "[Documentação do NetApp ONTAP](#)".
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Planilhas de cabeamento preenchidas. Consulte "[Preencha a planilha de cabeamento do Cisco Nexus 9336C-FX2](#)". Para mais informações sobre cabeamento, consulte o "[Hardware Universe](#)".

Passos

1. [[passo 3]]Realize uma configuração inicial dos switches.

Para a configuração, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches.

Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

2. Ligue o interruptor.

Ao ligar o switch pela primeira vez, forneça as respostas adequadas às seguintes perguntas de configuração inicial.

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 opção padrão é não.

- b. Deseja implementar um padrão de senhas seguras? (sim/não)

Responda com **sim**. A opção padrão é sim.

- c. Digite a senha de administrador.

A senha padrão é admin; você deve criar uma nova senha forte.

Uma senha fraca pode ser rejeitada.

d. Deseja acessar a caixa de diálogo de configuração básica? (sim/não)

Responda com **sim** na configuração inicial do switch.

e. Criar outra conta de login? (sim/não)

Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não.

f. Configurar string de comunidade SNMP somente leitura? (sim/não)

Responda com **não**. A opção padrão é não.

g. Configurar string de comunidade SNMP de leitura e gravação? (sim/não)

Responda com **não**. A opção padrão é não.

h. Digite o nome do interruptor.

O nome do interruptor está limitado a 63 caracteres alfanuméricos.

i. Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)

Responda com **sim** (a opção padrão) quando solicitado. No prompt "Endereço IPv4 mgmt0:", digite seu endereço IP: ip_address

j. Configurar o gateway padrão? (sim/não)

Responda com **sim**. No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.

k. Configurar opções avançadas de IP? (sim/não)

Responda com **não**. A opção padrão é não.

l. Habilitar o serviço Telnet? (sim/não)

Responda com **não**. A opção padrão é não.

m. Habilitar o serviço SSH? (sim/não)

Responda com **sim**. A opção padrão é sim.



Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.

a. Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1). O padrão é rsa.

b. Insira o número de bits da chave (1024-2048).

c. Configurar o servidor NTP? (sim/não)

Responda com **não**. A opção padrão é não.

d. Configurar a camada de interface padrão (L3/L2):

Responda com **L2**. O padrão é L2.

e. Configurar o estado padrão da interface da porta do switch (desligado/não desligado):

Responda com **noshut**. O padrão é noshut.

f. Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso):

Responda com **rigoroso**. O padrão é estrito.

g. Deseja editar a configuração? (sim/não)

Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com "não" quando solicitado, caso esteja satisfeito com a configuração. Responda com **sim** se desejar editar suas configurações.

h. Usar esta configuração e salvá-la? (sim/não)

Responda com **sim** para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.

3. Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.



Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito 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 compatível com a NetApp para os switches a partir do ["Download do software Cisco"](#) página.

O que vem a seguir?

Depois de configurar seus switches, você pode ["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 Arquivo de Configuração de Referência (RCF), siga este procedimento.

Documentação sugerida

- ["Página do switch Ethernet da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornecer informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são cs1 e cs2.
- Os nomes dos nós são cluster1-01 e cluster1-02.
- Os nomes LIF dos clusters são cluster1-01_clus1 e cluster1-01_clus2 para o cluster1-01 e cluster1-02_clus1 e cluster1-02_clus2 para o cluster1-02.
- O `cluster1::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(*>) aparece.

3. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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. Verifique o status administrativo ou operacional de cada interface do cluster e de cada porta de storage de nó e porta de storage de prateleira.

a. Exibir os atributos da porta de rede:

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

Mostrar exemplo

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

Node: cluster1-02

Health					Speed (Mbps)	
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

Health					Speed (Mbps)	
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
```

Current Vserver Port	Home	Logical Current Is Interface	Status Admin/Oper	Network Address/Mask	Node

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			
.					
.					

c. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

d. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

e. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::*> system switch ethernet show
Switch                                     Type                Address
Model
-----
s1
                                     storage-network      10.228.143.216
N9K-C9336C-FX2
  Serial Number: FDOXXXXXXB
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                     10.4(6)
  Version Source: CDP/ISDP

s2
                                     storage-network      10.228.143.219
N9K-C9336C-FX2
  Serial Number: FDOXXXXXXC
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                     10.6(2)
  Version Source: CDP/ISDP

cs1
                                     cluster-network      10.228.184.39
N9K-C9336C-FX2
  Serial Number: FLMXXXXXXXJ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                     10.4(6)
  Version Source: CDP/ISDP

cs2
                                     cluster-network      10.228.184.40
N9K-C9336C-FX2
```

```
Serial Number: FLMXXXXXXXXG
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
10.6(2)
Version Source: CDP/ISDP
```

5. Verifique a conectividade das interfaces do cluster remoto:

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

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

```

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				

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

1100


```

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. **[[passo 6]]** Verifique se o comando de reversão automática está habilitado 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
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

O que vem a seguir?

Após preparar a instalação do software NX-OS e do RCF, você pode ["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."](#) .

Requisitos de revisão

Antes de começar

Certifique-se de ter 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 da Cisco"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do 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 dos switches Cisco .

- ["Matriz de atualização e ISSU para Cisco Nexus 9000 e 3000"](#)

Fornecer informações sobre atualizações/downgrades disruptivos para o software Cisco NX-OS em switches da série Nexus 9000, com base nas versões atuais e desejadas.

Na página, selecione **Atualização disruptiva** e escolha a versão atual e a versão desejada na lista suspensa.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF dos clusters 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::*>` O prompt indica o nome do cluster.

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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. Exibir as portas do cluster em cada nó que estão conectadas 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				

4. Verifique o status administrativo e operacional de cada porta do cluster, porta de storage do nó e porta da prateleira de storage.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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					

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

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

Mostrar exemplo

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

Current	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			

c. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- d. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- e. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```


Mostrar exemplo

```
cluster1::*> system switch ethernet show
Switch                                     Type                Address
Model
-----
s1
                                     storage-network      10.228.143.216   N9K-
C9336C-FX2
    Serial Number: FDOXXXXXXB
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.4(6)
    Version Source: CDP/ISDP

s2
                                     storage-network      10.228.143.219   N9K-
C9336C-FX2
    Serial Number: FDOXXXXXXC
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.6(2)
    Version Source: CDP/ISDP

cs1
                                     cluster-network      10.228.184.39    N9K-
C9336C-FX2
    Serial Number: FLMXXXXXXXJ
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.4(6)
    Version Source: CDP/ISDP

cs2
                                     cluster-network      10.228.184.40    N9K-
C9336C-FX2
```

```
Serial Number: FLMXXXXXXXXG
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
10.6(2)
Version Source: CDP/ISDP
```

5. Desative a reversão automática nos LIFs do cluster. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 do software NX-OS em execução:

```
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 do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

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 após a reinicialização do switch:

```
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 all
```

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 de todas as portas do cluster.

- a. Verifique se as portas do cluster estão ativas e funcionando corretamente 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

Health	Health					Speed (Mbps)
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 o estado de saúde do switch 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
-----
-----
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
```

Você poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.
```

c. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- d. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- e. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```


Mostrar exemplo

```
cluster1::*> system switch ethernet show
```

Switch	Type	Address
Model		
-----	-----	-----
s1		
	storage-network	10.228.143.216 N9K-
C9336C-FX2		
Serial Number: FDOXXXXXXB		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.4(6)		
Version Source: CDP/ISDP		
s2		
	storage-network	10.228.143.219 N9K-
C9336C-FX2		
Serial Number: FDOXXXXXXC		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.6(2)		
Version Source: CDP/ISDP		
cs1		
	cluster-network	10.228.184.39 N9K-
C9336C-FX2		
Serial Number: FLMXXXXXXXJ		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.4(6)		
Version Source: CDP/ISDP		
cs2		
	cluster-network	10.228.184.40 N9K-
C9336C-FX2		

```
Serial Number: FLMXXXXXXXXG
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
10.6(2)
Version Source: CDP/ISDP
```

13. Verifique se o cluster está íntegro:

```
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 switch cs1.

15. Verifique a conectividade das interfaces do cluster remoto antes de ativar a reversão automática nas LIFs do cluster:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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		

Todas as versões do ONTAP

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

```
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. Ative a reversão automática nos LIFs do cluster.

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

2. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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		

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que vem a seguir?

Após instalar o software NX-OS, você pode ["instalar o RCF"](#).

Instale o arquivo de configuração de referência (RCF)

Você pode instalar o arquivo de configuração de referência (RCF) após 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 conexão de console com o switch. A conexão com o console é opcional se você tiver acesso remoto

ao switch.

- Os switches cs1 e cs2 estão ligados e a configuração inicial dos switches está concluída (o endereço IP de gerenciamento e o SSH estão configurados).
- A versão desejada do NX-OS foi instalada.
- As conexões entre switches (ISL) são estabelecidas.
- As portas do cluster de nós ONTAP não estão conectadas.

Configuração RCF disponível

- **ClusterStorageRCF** - Suporta um cluster particionado mais duas zonas de armazenamento nos switches (Cluster-Storage RCF 1.xx).

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch cs1 usando SSH ou usando um console serial.
2. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 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 do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas 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
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Registre quaisquer adições personalizadas entre o atual `running-config` arquivo e o arquivo RCF em uso.
7. Após verificar se as versões do 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. Reinicie o interruptor cs1.

```
cs1# reload
```

This command will reboot the system. (y/n)? [n] **y**

9. Repita as etapas de 1 a 8 no switch cs2.
10. Conecte as portas de cluster de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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 sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

3. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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#
```

Etapa 3: Configure seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager oferece um fluxo de trabalho simples e fácil para a configuração e instalação de clusters, incluindo a atribuição de um endereço IP de gerenciamento de nó, a inicialização do cluster, a criação de uma camada local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Vá para ["Configurar o ONTAP em um novo cluster com o System Manager"](#) Para obter instruções de configuração.

O que vem a seguir?

Após instalar o RCF, você pode ["configurar monitoramento de integridade do switch"](#).

Atualize seu arquivo de configuração de referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapa 1: Prepare-se para a atualização

1. Exibir as portas do cluster em cada nó que estão conectadas 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				

2. Verifique o status administrativo e operacional de cada porta do cluster, porta de storage do nó e porta da prateleira de storage.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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					

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

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

Mostrar exemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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			

c. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

- d. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

- e. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::*> system switch ethernet show
```

Switch	Type	Address
Model		
-----	-----	-----
s1		
	storage-network	10.228.143.216 N9K-
C9336C-FX2		
Serial Number: FDOXXXXXXB		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.4(6)		
Version Source: CDP/ISDP		
s2		
	storage-network	10.228.143.219 N9K-
C9336C-FX2		
Serial Number: FDOXXXXXXC		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.6(2)		
Version Source: CDP/ISDP		
cs1		
	cluster-network	10.228.184.39 N9K-
C9336C-FX2		
Serial Number: FLMXXXXXXXJ		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
10.4(6)		
Version Source: CDP/ISDP		
cs2		
	cluster-network	10.228.184.40 N9K-
C9336C-FX2		

```
Serial Number: FLMXXXXXXXXG
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
10.6(2)
Version Source: CDP/ISDP
```

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, desligue as portas conectadas às portas de cluster dos nós.

```
cs1(config)# interface eth1/1/1-2,eth1/7-8

cs1(config-if-range)# shutdown
```



Certifique-se de desligar **todas** as portas do cluster conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) para obter mais detalhes.

2. Verifique se as LIFs do cluster foram transferidas 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			

3. Verifique se o cluster está íntegro:

```
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. Caso ainda não o tenha feito, 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 a configuração em execução atual e o arquivo RCF em uso (como uma configuração SNMP para sua organização).
- b. Para NX-OS 10.2 e versões posteriores, use o `show diff running-config` comando para comparar com o arquivo RCF salvo na memória flash de inicialização. Caso contrário, utilize uma ferramenta de comparação ou de diferenças de terceiros.

5. Salve os detalhes básicos de 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 a versão 1.12 e posteriores do RCF, 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
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

7. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

8. Execute o comando `write erase` para apagar a configuração salva atualmente:

```
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 para a configuração de inicialização.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Execute um reinício do switch:

```
switch# reload
```

```
This command will reboot the system. (y/n)? [n] y
```


11. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

12. Copie o RCF para o bootflash do switch cs1 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 9000 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
```

14. Examine a saída do banner do `show banner motd` comando. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas 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
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

16. Reaplique quaisquer personalizações anteriores à configuração do switch.
17. Consulte "[Analise as considerações sobre cabeamento e configuração.](#)" para obter detalhes sobre quaisquer alterações adicionais necessárias.
18. Após verificar se as versões do RCF, as adições personalizadas e as configurações de interruptores estão corretas, copie o arquivo running-config para o arquivo startup-config.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na "[Guia de Comandos do Cisco Nexus Série 9000 NX-OS](#)".

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

19. Reinicie o interruptor cs1. Você pode ignorar os alertas do "monitor de integridade do switch de cluster" e os eventos de "portas de cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

20. Verifique a integridade de todas as portas do cluster.

- a. Verifique se as portas do cluster estão ativas e funcionando corretamente 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	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
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	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
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	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
Status	Status					
-----	-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

b. Verifique o estado de saúde do switch 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
-----
-----
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
```

Você poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.
```

c. Verifique se todas as portas de storage do nó estão ativas e com status íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

cluster1-01						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
cluster1-02						
	e5a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
.						
.						

d. Verifique se todas as portas da prateleira de armazenamento estão ativas e com status íntegro:

```
storage shelf port show
```

Mostrar exemplo

```
cluster1::> storage shelf port show
```

Shelf	ID	Module	State	Internal?

1.4				
	0	A	connected	false
	1	A	connected	false
	2	B	connected	false
	3	B	connected	false
.				
.				

e. Verifique se os switches estão sendo monitorados.

```
system switch ethernet show
```

Mostrar exemplo

```
cluster1::*> system switch ethernet show
Switch                                     Type                Address
Model
-----
s1
                                     storage-network      10.228.143.216   N9K-
C9336C-FX2
  Serial Number: FDOXXXXXXB
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.4(6)
  Version Source: CDP/ISDP

s2
                                     storage-network      10.228.143.219   N9K-
C9336C-FX2
  Serial Number: FDOXXXXXXC
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.6(2)
  Version Source: CDP/ISDP

cs1
                                     cluster-network      10.228.184.39    N9K-
C9336C-FX2
  Serial Number: FLMXXXXXXXJ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     10.4(6)
  Version Source: CDP/ISDP

cs2
                                     cluster-network      10.228.184.40    N9K-
C9336C-FX2
```



```
Serial Number: FLMXXXXXXXXG
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
10.6(2)
Version Source: CDP/ISDP
```

21. Verifique se o cluster está íntegro:

```
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::*>
```

22. Repita as etapas de 1 a 21 no switch cs2.

23. Ative a reversão automática nos LIFs do cluster.

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

Etapas 3: Verifique a configuração de rede do cluster e a integridade do cluster.

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 conectados:

```
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 do cluster estão em suas VLANs corretas usando os seguintes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar exemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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 sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

4. Verifique se a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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		

Se alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver vservice_name -lif lif_name
```

6. Verifique se o cluster está íntegro:

```
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

7. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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 vem a seguir?

Após atualizar o RCF, você pode ["configurar 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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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.

O que vem a seguir

Depois de reiniciar os interruptores, você pode ["reconfigurar"](#) eles conforme necessário.

Migrar switches

Migre de um cluster sem switch para armazenamento conectado diretamente.

Você pode migrar de um cluster sem switches com armazenamento conectado diretamente adicionando dois novos switches compartilhados.

O procedimento a ser utilizado depende de você ter 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 utilizam portas ópticas ou Twinax, mas não é suportado neste switch se os nós estiverem utilizando portas RJ45 10Gb BASE-T integradas para as portas de rede do cluster.

A maioria dos sistemas requer duas portas de rede dedicadas para cluster em cada controlador. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

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 switches Cisco Nexus 9336C-FX2 para permitir o dimensionamento

além de dois nós no cluster.

Requisitos de revisão

Assegure-se de que:

- Para a configuração sem switch de dois nós:
 - A configuração sem switch de dois nós está configurada corretamente e funcionando.
 - Os nós estão executando o ONTAP 9.8 ou posterior.
 - Todas as portas do cluster estão no estado **ativo**.
 - Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e em suas portas **principais**.
- Para a configuração do switch Cisco Nexus 9336C-FX2:
 - Ambos os switches possuem conectividade de rede de gerenciamento.
 - É possível acessar os switches do cluster através do console.
 - As conexões nó a nó e switch a switch do Nexus 9336C-FX2 usam cabos Twinax ou de fibra.
 - O "[Hardware Universe](#)" contém mais informações sobre cabeamento.
 - Os cabos Inter-Switch Link (ISL) são conectados às portas 1/35 e 1/36 em ambos os switches 9336C-FX2.
- A personalização inicial dos switches 9336C-FX2 foi concluída. Para que:
 - Os switches 9336C-FX2 estão executando a versão mais recente do software.
 - Os arquivos de configuração de referência (RCFs) foram aplicados aos switches.
 - Qualquer personalização do site, como SMTP, SNMP e SSH, é configurada nos novos switches.

Migre os switches

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- 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, respectivamente.
- O prompt `cluster1::*>` indica o nome do cluster.
- As portas de cluster usadas neste procedimento são *e3a* e *e3b*, conforme o controlador AFF A400. O "[Hardware Universe](#)" contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

Etapa 1: Migrar de um cluster sem switch com conexão direta

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`.

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

1. [[passo 2]]Altere o nível de privilégio para avançado, digitando "y" quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (*>) é exibida.

2. Desative todas as portas voltadas para os nós (exceto as portas ISL) nos dois novos switches do cluster, cs1 e cs2. Você não deve desativar as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra que as portas voltadas para o nó, de 1 a 34, 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. [[passo 4]]Verifique se o ISL e as portas físicas no ISL entre os dois switches 9336C-FX2 cs1 e cs2 estão ativos nas portas 1/35 e 1/36:

```
show port-channel summary
```

Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão ativas no switch 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 ativas no switch 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. [[passo 5]]Exibir a lista de dispositivos vizinhos:

```
show cdp neighbors
```


Este comando fornece informações sobre os dispositivos que estão conectados 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. [[passo 6]]Verifique se todas as portas do cluster estão ativas:

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

Cada porta deve exibir "Link ativo" e "Saudável" no status de integridade.

Mostrar exemplo

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

Node: node1

Health					Speed (Mbps)	
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

Health					Speed (Mbps)	
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. [[passo 7]]Verifique se todas as LIFs do cluster estão ativas e operacionais:

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

Cada LIF de cluster deve exibir verdadeiro para Is Home e ter um status Admin/Operador de ativo/ativo.

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. [[passo 8]]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. [[passo 9]]Desconecte o cabo da porta de cluster e3a no nó 1 e, em seguida, conecte e3a à porta 1 no switch de cluster cs1, usando o cabeamento apropriado compatível com os switches 9336C-FX2.

O "[Hardware Universe](#)" contém mais informações sobre cabeamento. Consulte "[Que informações adicionais preciso para instalar meu equipamento que não está no HWU?](#)" para obter mais informações sobre os requisitos de instalação do switch.

9. Desconecte o cabo da porta do cluster e3a no nó 2 e, em seguida, conecte e3a à porta 2 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
10. Habilite todas as portas voltadas para os nós no switch de cluster cs1.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão habilitadas 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 todos os LIFs do cluster estão **ativos**, operacionais e exibidos como verdadeiros para Is Home :

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

Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs estão **ativas** no nó 1 e no nó 2 e que Is Home Os resultados são **verdadeiros**:

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

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
true	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. Exibir informações sobre o estado 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. Desconecte o cabo da porta de cluster e3b no nó1 e, em seguida, conecte e3b à porta 1 no switch de cluster cs2, usando o cabeamento apropriado compatível com os switches 9336C-FX2.
14. Desconecte o cabo da porta do cluster e3b no nó 2 e, em seguida, conecte e3b à porta 2 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches 9336C-FX2.
15. Habilite todas as portas voltadas para os nós no switch de cluster cs2.

Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/34 estão habilitadas 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. [[passo 17]]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 ativas no nó 1 e no nó 2:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 exibem verdadeiro para Is Home :

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



Isso pode levar alguns minutos para ser concluído.

Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs estão **ativas** no nó 1 e no nó 2 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 com cada switch:

```
show cdp neighbors
```

Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
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. Exiba 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. [[passo 21]]Verifique se a configuração de armazenamento do par HA 1 (e do 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::*>
```

21. Verifique se as configurações estão desativadas:

```
network options switchless-cluster show
```



A conclusão do comando pode levar alguns minutos. Aguarde o anúncio de que o tempo de vida de 3 minutos está prestes a expirar.

O false O resultado no exemplo a seguir mostra que as configurações estão desativadas:

Mostrar exemplo

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. [[passo 23]]Verifique o status dos membros do nó no cluster:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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 administrador:

```
set -privilege admin
```

Passo 2: Configure o interruptor compartilhado

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 dos switches Cisco Nexus série 9000; os comandos ONTAP são usados, a menos que indicado de outra forma.

1. Verifique se a configuração de armazenamento do par HA 1 (e do 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 armazenamento estão íntegras e operacionais:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	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
node2						
30	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

3. [[passo 3]]Mova o par HA 1, portas do caminho A do NSM224 para o intervalo de portas sh1 11-22.
4. Instale um cabo do par HA 1, nó 1, caminho A para o intervalo de portas 11-22 do sh1. Por exemplo, o caminho de uma porta de armazenamento em um AFF A400 é e0c.
5. Instale um cabo do par HA 1, nó 2, caminho A para o intervalo de portas 11-22 do sh1.
6. 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	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	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
node2						
30	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

7. Verifique se não há problemas com os switches de armazenamento ou com a fiação do cluster:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

8. Mova as portas do caminho B do par HA 1 do NSM224 para o intervalo de portas 11-22 do sh2.
9. Instale um cabo do par HA 1, nó 1, caminho B para o intervalo de portas 11-22 do sh2. Por exemplo, a porta de armazenamento do caminho B em um AFF A400 é e5b.
10. Instale um cabo do par HA 1, nó 2, caminho B para o intervalo de portas 11-22 do sh2.

11. 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
```

VLAN					Speed		
Node	Port	Type	Mode	(Gb/s)	State	Status	
ID							

node1							
30	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	
node2							
30	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	

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 armazenamento secundário (controlador) não utilizadas no par HA 1, alterando-as de armazenamento para rede. Se mais de um NS224 estiver conectado diretamente, haverá portas que precisarão 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 desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migre de uma configuração comutada para armazenamento conectado diretamente.

Você pode migrar de uma configuração comutada com armazenamento conectado diretamente adicionando dois novos switches compartilhados.

Interruptores suportados

Os seguintes interruptores são suportados:

- Nexus 9336C-FX2
- Nexus 3232C

As versões do ONTAP e do NX-OS suportadas neste procedimento estão na página Cisco Ethernet Switches. Consulte ["Switches Ethernet da Cisco"](#).

Portas de conexão

Os switches utilizam as seguintes portas para se conectar aos nós:

- Nexus 9336C-FX2:
 - Portas 1-3: Modo Breakout (4x10G) Portas Intra-Cluster, int e1/1/1-4, e1/2/1-4, e1/3/1-4
 - Portas 4-6: Modo breakout (4x25G) Portas intra-cluster/HA, 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 3232C:
 - Portas 1-30: 10/40/100 GbE
- Os switches utilizam as seguintes portas de Interconexão entre Switches (ISL):
 - Portas int e1/35-36: Nexus 9336C-FX2
 - Portas e1/31-32: Nexus 3232C

O ["Hardware Universe"](#) documento contém informações sobre a cablagem suportada para todos os switches de cluster.

O que você vai precisar

- Certifique-se de ter concluído as seguintes tarefas:
 - Configurei algumas portas nos switches Nexus 9336C-FX2 para funcionarem em 100 GbE.
 - Planejamos, migramos e documentamos a conectividade de 100 GbE dos nós para os switches Nexus 9336C-FX2.
 - Migrei, sem interrupções, outros switches de cluster Cisco de um cluster ONTAP para switches de rede Cisco Nexus 9336C-FX2.
- A rede de switches existente está configurada corretamente e funcionando.

- Todas as portas estão em estado **ativo** para garantir operações sem interrupções.
- Os switches Nexus 9336C-FX2 estão configurados e operando com a versão correta do NX-OS instalada e o arquivo de configuração de referência (RCF) aplicado.
- A configuração de rede existente apresenta as seguintes características:
 - Um cluster NetApp redundante e totalmente funcional, utilizando switches Cisco mais antigos.
 - Conectividade de gerenciamento e acesso ao console tanto para os switches Cisco mais antigos quanto para os novos.
 - Todas as LIFs do cluster estão no estado **ativo** e conectadas às suas portas de origem.
 - As portas ISL foram habilitadas e conectadas por cabos entre os outros switches Cisco e entre os novos switches.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster são *node1_clus1* e *node1_clus2* no nó 1, e *node2_clus1* e *node2_clus2* no nó 2, respectivamente.
- O interruptor *c2* é substituído primeiro pelo interruptor *sh2* e, em seguida, o interruptor *c1* é substituído pelo interruptor *sh1*.

Passos

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

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

Onde x representa a duração do período de manutenção em horas.

2. Verifique o status administrativo e operacional de cada porta do cluster.
3. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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. [[passo 4]]Verifique se todas as interfaces de cluster (LIFs) estão na porta principal:

```
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. [[passo 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. [[passo 6]]Desative a reversão automática nos LIFs do cluster.

Mostrar exemplo

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

7. [[passo 7]]Desligue o interruptor 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. [[passo 8]]Verifique se as LIFs do 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. [[passo 9]]Substitua o interruptor c2 pelo novo interruptor sh2 e reconecte os cabos do novo interruptor.
10. Verifique se as portas estão novamente ativas no sh2. **Observação:** os LIFs ainda estão no switch c1.
11. Desligue o interruptor 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 do cluster migraram para as portas hospedadas no switch de cluster sh2. Isso pode levar alguns segundos.

Mostrar exemplo

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

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

Cluster					
true	node1_clus1	up/up	169.254.3.4/23	node1	e3a
false	node1_clus2	up/up	169.254.3.5/23	node1	e3a
true	node2_clus1	up/up	169.254.3.8/23	node2	e3a
false	node2_clus2	up/up	169.254.3.9/23	node2	e3a

4 entries were displayed.
cluster1::*>

13. Substitua o interruptor c1 pelo novo interruptor sh1 e reconecte os cabos do novo interruptor.
14. Verifique se as portas estão novamente ativas no sh1. **Observação:** os LIFs ainda estão no switch c2.
15. Ativar reversão automática nos LIFs do cluster:

Mostrar exemplo

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

16. Verifique se o cluster está íntegro:

```
cluster show
```

Mostrar exemplo

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      false
node2          true   true      false
2 entries were displayed.
cluster1::*>
```

O que vem a seguir?

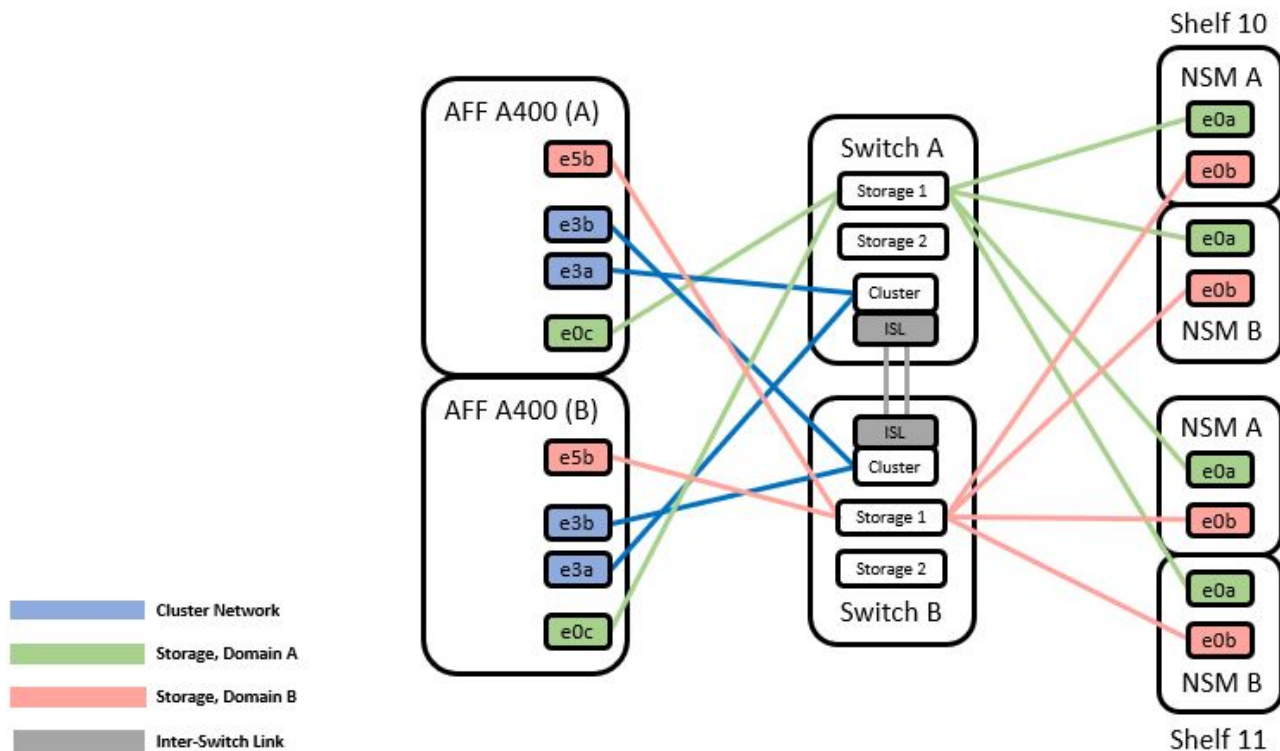
Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migre de uma configuração sem switches com armazenamento conectado a switches reutilizando os switches de armazenamento.

Você pode migrar de uma configuração sem switches para um armazenamento conectado a switches reutilizando os switches de armazenamento.

Ao reutilizar os switches de armazenamento, os switches de armazenamento do par HA 1 tornam-se os switches compartilhados, conforme mostrado na figura a seguir.

Switch Attached



Passos

1. Verifique se a configuração de armazenamento do par HA 1 (e do 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. [[passo 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	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						
-----	-----	-----	-----	-----	-----	-----
node1						
30	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
node2						
30	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

3. [[passo 3]]Mova os cabos do par HA 1, caminho A do NSM224 do switch de armazenamento A para as portas de armazenamento NS224 compartilhadas para o par HA 1, caminho A no switch de armazenamento A.
4. Mova o cabo do par HA 1, nó A, caminho A para a porta de armazenamento compartilhada do par HA 1, nó A no switch de armazenamento A.
5. Mova o cabo do par HA 1, nó B, caminho A para a porta de armazenamento compartilhada do par HA 1, nó B no switch de armazenamento A.
6. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento A, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

7. [[passo 7]]Substitua o RCF de armazenamento no switch compartilhado A pelo arquivo RCF compartilhado. Consulte "[Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2.](#)" para obter mais detalhes.
8. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento B, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

9. [[passo 9]]Mova os cabos do par HA 1, caminho B do NSM224 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 HA 1, nó A, caminho B para a porta de armazenamento compartilhada do par HA 1, nó A, caminho B no switch de armazenamento B.
11. Mova o cabo do par HA 1, nó B, caminho B para a porta de armazenamento compartilhada do par HA 1, nó B, caminho B no switch de armazenamento B.
12. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento B, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

13. [[passo 13]]Substitua o arquivo RCF de armazenamento no switch compartilhado B pelo arquivo RCF compartilhado. Consulte "[Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2.](#)" para obter mais detalhes.
14. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento B, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

15. [[passo 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 de HA 1 de um cluster sem switch para um cluster com switch. Use as atribuições de porta do cluster definidas pelo RCF compartilhado. Consulte ["Instale o software NX-OS e os arquivos de configuração de referência \(RCFs\)"](#) para obter mais detalhes.
17. Verifique se a configuração de rede comutada é válida:

```
network port show
```

O que vem a seguir?

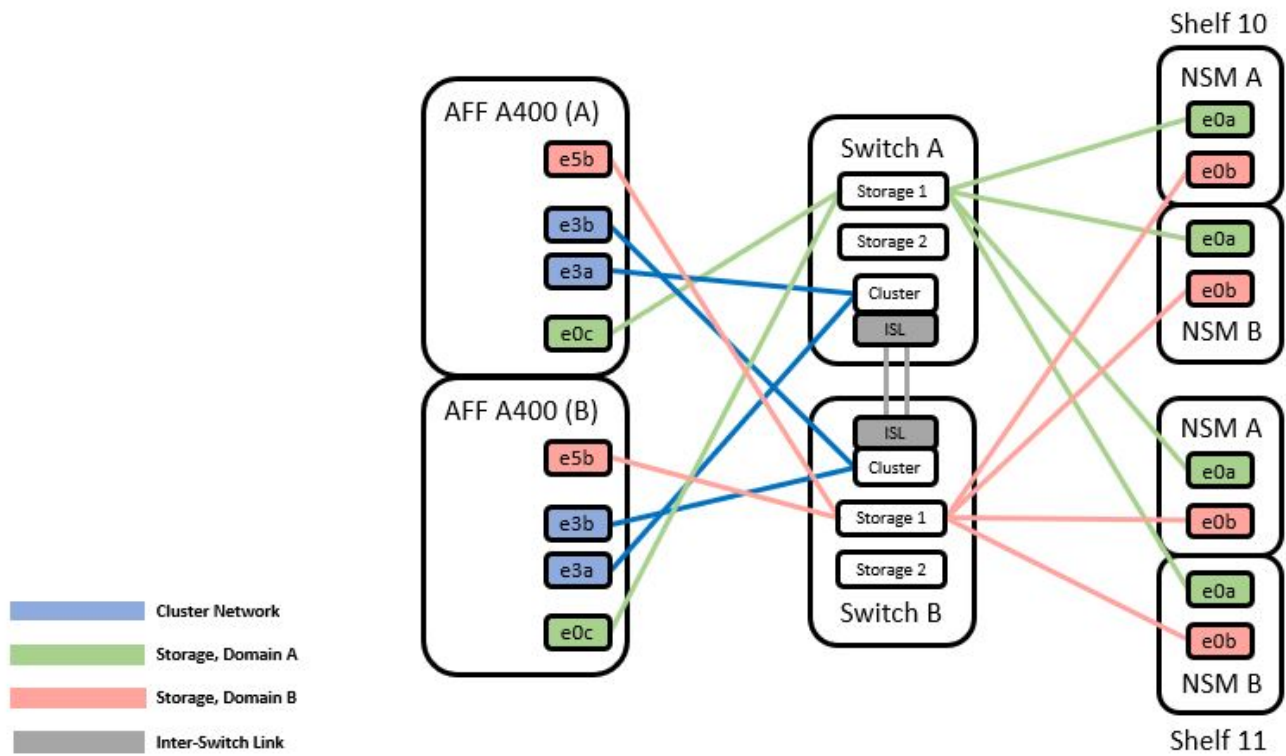
Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Migrar de um cluster comutado com armazenamento conectado ao switch

É possível migrar de um cluster comutado com armazenamento conectado ao switch reutilizando os switches de armazenamento.

Ao reutilizar os switches de armazenamento, os switches de armazenamento do par HA 1 tornam-se os switches compartilhados, conforme mostrado na figura a seguir.

Switch Attached



Passos

1. Verifique se a configuração de armazenamento do par HA 1 (e do 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. [[passo 2]]Mova os cabos do par HA 1, caminho A do NSM224 do switch de armazenamento A para as portas de armazenamento do NSM224 para o par HA 1, caminho A no switch de armazenamento A.
3. Mova o cabo do par HA 1, nó A, caminho A para a porta de armazenamento NSM224 do par HA 1, nó A no switch de armazenamento A.
4. Mova o cabo do par HA 1, nó B, caminho A para a porta de armazenamento NSM224 do par HA 1, nó B no switch de armazenamento A.
5. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento A, está íntegro:

```
storage port show -port-type ENET
```


Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	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
node2						
30	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

6. [[passo 6]]Substitua o RCF de armazenamento no switch compartilhado A pelo arquivo RCF compartilhado. Consulte "[Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2.](#)" para obter mais detalhes.
7. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento A, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance
```

```
There are no entries matching your query.
```

8. [[passo 8]]Mova os cabos do par HA 1, caminho B do NSM224 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 HA 1, nó A, caminho B para a porta de armazenamento compartilhada do par HA 1, nó A, caminho B no switch de armazenamento B.
10. Mova o cabo do par HA 1, nó B, caminho B para a porta de armazenamento compartilhada do par HA 1, nó B, caminho B no switch de armazenamento B.
11. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento B, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

12. [[passo 12]]Substitua o arquivo RCF de armazenamento no switch compartilhado B pelo arquivo RCF compartilhado. Consulte "[Instale o RCF em um switch compartilhado Cisco Nexus 9336C-FX2.](#)" para mais detalhes.
13. Verifique se o armazenamento conectado ao par HA 1, switch de armazenamento B, está íntegro:

```
system health alert show -instance
```

Mostrar exemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

14. [[passo 14]]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::*>
```

15. [[passo 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 de cluster dos switches de cluster existentes para os switches compartilhados usando o procedimento de substituição de switch e o RCF compartilhado. O novo switch compartilhado A é "cs1". O novo switch compartilhado B é "cs2". Consulte ["Substitua um switch compartilhado Cisco Nexus 9336C-FX2"](#) 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. Remova os interruptores de cluster não utilizados.
19. Remova os interruptores de armazenamento não utilizados.

O que vem a seguir?

Depois de migrar seus switches, você pode ["configurar monitoramento de integridade do switch"](#).

Substitua um switch compartilhado Cisco Nexus 9336C-FX2

Você pode substituir um switch compartilhado Nexus 9336C-FX2 defeituoso. Este é um procedimento não disruptivo (NDU).

Antes de começar

Antes de substituir o interruptor, certifique-se de que:

- Na infraestrutura de cluster e rede existente:
 - O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
 - Todas as portas do cluster estão **ativas**.
 - Todas as interfaces lógicas do cluster (LIFs) estão **ativas** e em suas portas de origem.
 - O comando `ping-cluster -node node1` do cluster ONTAP deve indicar que a conectividade

básica e a comunicação com largura de banda superior a PMTU estão funcionando corretamente em todos os caminhos.

- Para o interruptor de substituição Nexus 9336C-FX2:
 - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - As conexões de nó são as portas 1/1 a 1/34:
 - Todas as portas de Interconexão de Switches (ISL) estão desativadas nas portas 1/35 e 1/36.
 - O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional NX-OS são carregados no switch.
 - Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, devem ser copiadas para o novo switch.

Sobre os exemplos

Você deve executar o comando para migrar um LIF de cluster a partir do nó onde o LIF de cluster está hospedado.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos switches Nexus 9336C-FX2 existentes são *sh1* e *sh2*.
- Os nomes dos novos switches Nexus 9336C-FX2 são *newsh1* e *newsh2*.
- Os nomes dos nós são *node1* e *node2*.
- As portas do cluster em cada nó são denominadas *e3a* e *e3b*.
- Os nomes 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 para alterações em todos os nós do cluster é *cluster1::*>*.



O procedimento a seguir 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
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, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

Onde x representa a duração do período de manutenção em horas.

2. Opcional: Instale o RCF e a imagem apropriados no switch, newsh2, e faça todos os preparativos necessários no local.
 - a. Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e NX-OS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e NX-OS, prossiga para [Passo 3](#) .
 - b. Acesse a página de descrição do arquivo de configuração de referência dos switches de cluster e de rede de gerenciamento da NetApp no site de suporte da NetApp .
 - c. Clique no link para a Matriz de Compatibilidade de Rede de Cluster e Rede de Gerenciamento e, em seguida, observe a versão de software do switch necessária.
 - d. Clique na seta "Voltar" do seu navegador para retornar à página de Descrição, clique em CONTINUAR, aceite o contrato de licença e, em seguida, acesse a página de Download.
 - e. Siga os passos na página de Download para baixar os arquivos RCF e NX-OS corretos para a versão do software ONTAP que você está instalando.
3. [\[\[passo 3\]\]](#)No novo switch, faça login como administrador e desligue todas as portas que serão conectadas às interfaces do cluster de nós (portas 1/1 a 1/34). Se o interruptor que você está substituindo não estiver funcionando e estiver desligado, vá para [Passo 4](#) . As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em 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. [\[\[passo 4\]\]](#)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. [[passo 5]] Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 6]]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. [[passo 7]]Remova todos os cabos do switch Nexus 9336C-FX2 sh2 e, em seguida, conecte-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, em seguida, verifique o status da operação do canal da porta.

Port-Channel deve indicar Po1(SU) e Member Ports deve indicar Eth1/35(P) e Eth1/36(P).

Mostrar exemplo

Este exemplo habilita as portas ISL 1/35 e 1/36 e exibe o resumo do canal de 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. [[passo 9]]Verifique se a porta e3b está ativa em todos os nós:

```
network port show ipspace Cluster
```

Mostrar exemplo

O resultado deverá ser semelhante ao seguinte:

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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 do cluster associado à porta na etapa anterior usando o comando de reversão da interface de rede.

Neste exemplo, a LIF node1_clus2 no nó 1 é revertida com sucesso se o valor de Home for verdadeiro e a porta for e3b.

Os comandos a seguir retornam o LIF node1_clus2 no nó 1 para a porta home e3a e exibem informações sobre os LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se a coluna "Is Home" estiver definida como **verdadeira** para ambas as interfaces do cluster e se elas exibirem as atribuições de porta corretas, neste exemplo, e3a e e3b no nó 1.

Mostrar exemplo

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e3b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e3a	node2_clus2	up/up	169.254.19.183/16	node2
	false			
4 entries were displayed.				

6. Exibir informações sobre os nós em um cluster:

```
cluster show
```

Mostrar exemplo

Este exemplo mostra que o estado de saúde dos nós node1 e node2 neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

Node	Health	Eligibility

node1	false	true
node2	true	true

7. [[passo 12]]Verifique se todas as portas físicas 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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

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. [[passo 13]] Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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. **[[passo 14]]** Confirme a seguinte configuração de rede do 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 switch antigo sh2 para o novo switch newsh2.
- 3. Verifique se o armazenamento conectado ao par HA 1, switch compartilhado newsh2, está íntegro.
- 4. Verifique se o armazenamento conectado ao par HA 2, switch compartilhado newsh2, está íntegro:

```
storage port show -port-type ENET
```

Mostrar exemplo

```
storage::*> storage port show -port-type ENET
```

Speed

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						

node1						
30	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
node2						
30	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

5. [[passo 18]]Verifique se as prateleiras estão corretamente cabeadas:

```
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 interruptor antigo sh2.
7. Repita esses passos para o switch sh1 e para o novo switch newsh1.
8. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir os interruptores, você pode ["configurar monitoramento de integridade do switch"](#).

Monitorar o estado do interruptor

Visão geral do monitor de integridade do switch

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração.

Configure o monitoramento de integridade do switch.

Visão geral da configuração

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração.

- ["Configurar coleta de logs"](#)
- ["Configurar SNMPv3 \(Opcional\)"](#)

Configurar coleta de logs

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração. Este procedimento orienta você no processo de configuração da coleta, solicitação de registros detalhados de **Suporte** e ativação da coleta horária de dados **Periódicos** coletados pelo AutoSupport.

NOTA: Se você ativar o modo FIPS, deverá concluir o seguinte:



1. Recrie as chaves SSH no switch seguindo as instruções do fornecedor.
2. Regenerar chaves SSH no ONTAP usando `debug system regenerate-systemshell-key-pair`
3. Execute novamente a rotina de configuração de coleta de logs usando o `system switch ethernet log setup-password` comando

Antes de começar

- O usuário deve ter acesso ao interruptor. `show` comandos. Caso essas opções não estejam disponíveis, crie um novo usuário e conceda as permissões necessárias a ele.
- O monitoramento de integridade do switch deve estar ativado. Verifique isso certificando-se de que `Is Monitored:` O campo é definido como **verdadeiro** 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 coleta de logs

habilitada. Esses switches não suportam múltiplas chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleta de logs realizada sobrescreverá quaisquer chaves SSH preexistentes do usuário.

- Para suporte à coleta de logs com switches NVIDIA , o *usuário* responsável pela coleta de logs deve ter permissão para executar o comando. `cl-support` comando sem precisar 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 coleta de logs, execute o seguinte comando para cada switch. Você será solicitado a inserir o nome do switch, o nome de usuário e a senha para a coleta de logs.

NOTA: Se responder **s** à solicitação 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** à seguinte mensagem: Deseja especificar um usuário diferente de admin para a coleta de logs? {s|n}: **s**

1. [[passo 2]]Ativar a 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 suporte para coleta de registros:

```
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 visualizar todos os detalhes da coleta de logs, incluindo a ativação, a mensagem de status, o carimbo de data/hora anterior e o nome do arquivo da coleta periódica, bem como o status da solicitação, a mensagem de status e o carimbo de data/hora anterior e o nome do arquivo da coleta de suporte, utilize o seguinte comando:

```
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 coleta de logs, execute o seguinte comando para cada switch. Você será solicitado a inserir o nome do switch, o nome de usuário e a senha para a coleta de logs.

NOTA: Se responder y Na solicitação 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** à seguinte mensagem: Deseja especificar um usuário diferente de admin para a coleta de logs? {s|n}: **s**

1. [[passo 2]] Para solicitar a coleta de logs de suporte e habilitar a coleta periódica, execute o seguinte comando. Isso inicia os dois tipos de coleta de logs: a detalhada Support registros e uma coleta horária de Periodic dados.

```
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 verifique se a coleta de logs foi concluída:

```
system switch ethernet log show
```



Se algum status de erro for relatado pelo recurso de coleta de logs (visível na saída de `system switch ethernet log show`), consulte ["Solução de problemas na coleta de logs"](#) para obter mais detalhes.

O que vem a seguir?

["Configurar SNMPv3 \(Opcional\)"](#).

Configure o SNMPv3 para o seu switch (Opcional)

O SNMP é usado para monitorar os switches. O monitoramento por SNMPv3 é configurado seguindo este procedimento.

O Ethernet Switch Health Monitor (CSHM) utiliza SNMP para monitorar a integridade e o desempenho de switches de cluster e de armazenamento. Por padrão, o SNMPv2c é configurado automaticamente através do Arquivo de Configuração de Referência (RCF). O SNMPv3 é mais seguro 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 compatível com o ONTAP 9.12.1 e versões posteriores.
- O ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 e versões posteriores corrigem esses dois problemas:
 - "Para monitoramento de integridade do ONTAP em switches Cisco , o tráfego SNMPv2 ainda pode ser observado após a migração para o SNMPv3."
 - "Alertas falsos positivos de ventoinha e energia do switch quando ocorrem falhas SNMP."

Sobre esta tarefa

Os seguintes comandos são usados para configurar um nome de usuário SNMPv3 em switches **Broadcom**, * Cisco* e * NVIDIA*:

switches Broadcom

Configure um nome de usuário SNMPv3 NETWORK-OPERATOR em switches Broadcom BES-53248.

- Para **nenhuma autenticação**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp  
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

2. Configure o usuário SNMPv3 no lado do 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: cshml!
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 consulta do CSHM, verifique se o número de série está preenchido para o switch Ethernet.

```
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, nos switches Cisco 9336C-FX2:

- Para **nenhuma autenticação**:

```
snmp-server user SNMPv3_USER NoAuth
```

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 do 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: cshml!
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 detalhado na etapa anterior, após a conclusão do período de pesquisa CSHM.

```
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 a CLI 5.4.0:

- Para **nenhuma autenticação**:

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 laErrorMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```



```

pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syservices 72
-rocommunity cshml! default

```

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

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username SNMPv3User auth-md5 <password> encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames      Configured    <---- Configured
here
-----

```

```

cumulus@sw1:~$

```

2. Configure o usuário SNMPv3 no lado do ONTAP :

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-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 detalhado na etapa anterior, após a conclusão do período de pesquisa CSHM.

```
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 a CLI 5.11.0:

- Para **nenhuma autenticação**:

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 do ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configure o CSHM para monitorar com o novo usuário SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 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 detalhado na etapa anterior, após a conclusão do período de pesquisa CSHM.

```
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 o estado do interruptor.

Visão geral do check-up de saúde

Os monitores de integridade monitoram proativamente determinadas condições críticas em seu cluster e emitem alertas caso detectem uma falha ou risco.

Para visualizar os alertas de monitoramento de integridade do switch Ethernet atualmente em execução, execute o comando: `system health alert show -monitor ethernet-switch`

Para visualizar 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 descobertos automaticamente pelo ONTAP e monitorados pelo CSHM. O arquivo de configuração de referência (RCF) aplicado ao switch, entre outras coisas, habilita o Cisco Discovery Protocol (CDP) e/ou o Link Layer Discovery Protocol (LLDP). No entanto, pode ser necessário adicionar manualmente um interruptor que não foi detectado ou remover um interruptor que não

está mais em uso. Você também pode interromper o monitoramento ativo, mantendo o switch na configuração, por exemplo, durante a manutenção.

Crie uma entrada de interruptor 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 específico. Isso é útil caso o ONTAP não adicione o switch automaticamente ou se você o removeu anteriormente e deseja adicioná-lo novamente.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshml! -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 **cshml!**. Usar `-type storage-network` em vez de `-type cluster-network` Se você estiver configurando um switch de armazenamento.

Desative o monitoramento sem excluir o interruptor.

Se você deseja pausar ou interromper o monitoramento de um determinado switch, mas ainda mantê-lo para monitoramento futuro, modifique-o. `is-monitoring-enabled-admin` parâmetro em vez de excluí-lo.

Por exemplo:

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Isso permite preservar os detalhes e a configuração do switch sem gerar novos alertas ou redescobertas.

Remova um interruptor que você não precisa mais.

Usar `system switch ethernet delete` Para excluir um interruptor que foi desconectado ou não é mais necessário:

```
system switch ethernet delete -device DeviceName
```

Por padrão, este comando só terá sucesso se o ONTAP não detectar o switch por meio de CDP ou LLDP. Para remover um interruptor detectado, use o `-force` parâmetro:

```
system switch ethernet delete -device DeviceName -force
```

Quando `-force` Se o ONTAP o detectar novamente, ele poderá ser adicionado novamente de forma automática.

Verifique o monitoramento dos switches Ethernet.

O monitor de integridade do switch Ethernet (CSHM) tenta monitorar automaticamente os switches que detecta; no entanto, o monitoramento pode não ocorrer automaticamente se os switches não estiverem configurados corretamente. Você deve verificar se o monitor de integridade está configurado corretamente para monitorar seus switches.

Confirme o monitoramento dos switches Ethernet conectados.

Para confirmar se os switches Ethernet conectados estão sendo monitorados, execute o seguinte comando:

```
system switch ethernet show
```

Se o `Model A` coluna exibe **OUTRO** ou o `IS Monitored` Se o campo exibir **false**, o ONTAP não poderá monitorar o switch. Um valor de **OUTRO** normalmente indica que o ONTAP não suporta essa opção para monitoramento de integridade.

O `IS Monitored` O campo está definido como **falso** pelo motivo especificado no `Reason` campo.



Se um switch não estiver listado na saída do comando, é provável que o ONTAP ainda não o tenha detectado. Confirme se o interruptor está conectado corretamente. Se necessário, você pode adicionar o interruptor manualmente. Ver ["Gerenciar o monitoramento de switches Ethernet"](#) Para obter mais detalhes.

Confirme se as versões do firmware e do RCF estão atualizadas.

Certifique-se de que o switch esteja executando o firmware mais recente compatível e que um arquivo de configuração de referência (RCF) compatível tenha sido aplicado. Mais informações estão disponíveis em <https://mysupport.netapp.com/site/downloads>["Página de downloads de suporte da NetApp"] .

Por padrão, o monitor de integridade usa SNMPv2c com a string de comunidade **cshm1!** para monitoramento, mas o SNMPv3 também pode ser configurado.

Se precisar alterar a string de comunidade SNMPv2c padrão, certifique-se de que a string de comunidade SNMPv2c desejada esteja configurada no switch.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c  
-community-or-username newCommunity!
```



Ver ["Opcional: Configurar SNMPv3"](#) Para obter detalhes sobre como configurar o SNMPv3 para uso.

Confirme a conexão da rede de gerenciamento.

Verifique se a porta de gerenciamento do switch está conectada à rede de gerenciamento.

Para que o ONTAP execute consultas SNMP e colete logs, é necessária uma conexão correta à porta de

gerenciamento.

Solucionar problemas de alertas

Os alertas são gerados se uma falha, risco ou condição crítica for detectada em um switch Ethernet do seu cluster.

Caso sejam acionados alertas, o status de integridade do sistema será relatado como degradado para o cluster. Os alertas gerados incluem as informações necessárias para que você possa responder à degradação da integridade do sistema.

Para visualizar 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 Knowledge Base ["Guia de Resolução de Alertas do Monitor de Saúde do Switch"](#) para obter detalhes avançados sobre a resolução de alertas.

Coleta de registros

Visão geral da coleta de logs

Com a coleta de logs configurada, você pode habilitar a coleta horária de dados periódicos que são coletados pelo AutoSupport e solicitar logs de suporte detalhados.

Consulte ["Configurar coleta de logs"](#) para obter mais detalhes.

Solução de problemas na coleta de logs

Se você encontrar algum dos seguintes códigos de erro relatados pelo recurso de coleta de logs (visíveis na saída do `system switch ethernet log show` comando), tente as etapas de depuração correspondentes:

Status de erro na coleta de logs	Resolução
Chaves RSA não presentes	Regenerar as chaves SSH do ONTAP .
Erro na senha do switch	Verificar credenciais, testar a conectividade SSH e regenerar as chaves SSH do ONTAP . Consulte a documentação do switch ou entre em contato com 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 no switch antes de tentar novamente.
Registro pré-existente encontrado	Remova o arquivo de coleta de logs anterior no switch.

Erro no log de despejo do switch

Certifique-se de que o usuário do switch tenha permissões de coleta de logs. Consulte os pré-requisitos acima.



Se as instruções de resolução não funcionarem, entre em contato com o suporte da NetApp .

Interruptores de fim de disponibilidade

Interruptores de fim de 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 vendas e fim de vida útil

- ["Anúncio de Fim de Vendas e Fim de Vida Útil do Cisco Nexus 3232C"](#)
- ["Anúncio de Fim de Vendas e Fim de Vida Útil para os modelos Cisco Nexus 31108PC-V, 31108TC-V e Nexus 3132Q-V"](#)
- ["Anúncio de Fim de Vendas e Fim de Vida Útil para os Cisco N9K-C93120TX e N9K-C92300YC"](#)
- ["Anúncio de Fim de Vendas e Fim de Vida Útil para os Switches Cisco Nexus Série 5500"](#)
- ["Fim da disponibilidade: SKUs de interconexão de cluster NetApp CN1610"](#)

Cisco Nexus 3232C

Começar

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 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 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.



"Instale o hardware"

Instale o hardware do switch.



"Configurar o software"

Configure o software do switch.

Requisitos de configuração para switches Cisco Nexus 3232C

Para instalação e manutenção do switch Cisco Nexus 3232C, certifique-se de revisar os requisitos de configuração e de rede.

Requisitos de configuração

Para configurar seu cluster, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches. Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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.

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter as informações mais recentes.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

O que vem a seguir

Após confirmar os requisitos de configuração, você poderá revisar o ["documentação necessária"](#).

Requisitos de documentação para switches Cisco Nexus 3232C

Para a instalação do switch Cisco Nexus 3232C, certifique-se de revisar toda a documentação recomendada.

Documentação do Switch

Para configurar os switches Cisco Nexus 3232C, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 3000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 3000</i>	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 3000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 3000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 3000 Series NX-OS</i>	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 3000</i>	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 3000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 3000</i>	Descreve as mensagens do sistema para switches da série Cisco Nexus 3000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
Notas de versão do NX-OS para a série Cisco Nexus 3000 (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 3000.
Informações regulamentares, de conformidade e de segurança para os Cisco Nexus 6000, Cisco Nexus série 5000, Cisco Nexus série 3000 e Cisco Nexus série 2000.	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 3000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornecer informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco 3232C em um NetApp cabinet, consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"Instale um switch Cisco Nexus 3232C em um gabinete NetApp ."	Este manual descreve como instalar um switch Cisco Nexus 3232C em um gabinete NetApp de quatro postes.

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale o switch 3232C.

3

"Instale o switch em um gabinete NetApp."

Instale o switch 3232C e o painel de passagem em um gabinete NetApp , conforme necessário.

4

"Revisar a cablagem e a configuração."

Revise o suporte para portas Ethernet NVIDIA .

Folha de exercícios completa de cabeamento do Cisco Nexus 3232C

Se você deseja documentar as plataformas suportadas, baixe o PDF desta página e preencha a planilha de cabeamento.

A planilha de cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

Cada switch pode ser configurado como uma única porta 100GbE, uma porta 40GbE ou quatro portas 10GbE.

Exemplo de folha de exercícios de cabeamento

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 4x10GbE/4x25GbE ou 40/100GbE	1	Nó 4x10GbE/4x25GbE ou 40/100GbE
2	Nó 4x10GbE/4x25GbE ou 40/100GbE	2	Nó 4x10GbE/4x25GbE ou 40/100GbE
3	Nó 4x10GbE/4x25GbE ou 40/100GbE	3	Nó 4x10GbE/4x25GbE ou 40/100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
4	Nó 4x10GbE/4x25GbE ou 40/100GbE	4	Nó 4x10GbE/4x25GbE ou 40/100GbE
5	Nó 4x10GbE/4x25GbE ou 40/100GbE	5	Nó 4x10GbE/4x25GbE ou 40/100GbE
6	Nó 4x10GbE/4x25GbE ou 40/100GbE	6	Nó 4x10GbE/4x25GbE ou 40/100GbE
7	Nó 4x10GbE/4x25GbE ou 40/100GbE	7	Nó 4x10GbE/4x25GbE ou 40/100GbE
8	Nó 4x10GbE/4x25GbE ou 40/100GbE	8	Nó 4x10GbE/4x25GbE ou 40/100GbE
9	Nó 4x10GbE/4x25GbE ou 40/100GbE	9	Nó 4x10GbE/4x25GbE ou 40/100GbE
10	Nó 4x10GbE/4x25GbE ou 40/100GbE	10	Nó 4x10GbE/4x25GbE ou 40/100GbE
11	Nó 4x10GbE/4x25GbE ou 40/100GbE	11	Nó 4x10GbE/4x25GbE ou 40/100GbE
12	Nó 4x10GbE/4x25GbE ou 40/100GbE	12	Nó 4x10GbE/4x25GbE ou 40/100GbE
13	Nó 4x10GbE/4x25GbE ou 40/100GbE	13	Nó 4x10GbE/4x25GbE ou 40/100GbE
14	Nó 4x10GbE/4x25GbE ou 40/100GbE	14	Nó 4x10GbE/4x25GbE ou 40/100GbE
15	Nó 4x10GbE/4x25GbE ou 40/100GbE	15	Nó 4x10GbE/4x25GbE ou 40/100GbE
16	Nó 4x10GbE/4x25GbE ou 40/100GbE	16	Nó 4x10GbE/4x25GbE ou 40/100GbE
17	Nó 4x10GbE/4x25GbE ou 40/100GbE	17	Nó 4x10GbE/4x25GbE ou 40/100GbE
18	Nó 4x10GbE/4x25GbE ou 40/100GbE	18	Nó 4x10GbE/4x25GbE ou 40/100GbE

Chave seletora de cluster A		Chave seletora de cluster B	
19	Nó 19 de 40G/100GbE	19	Nó 19 de 40G/100GbE
20	Nó 20 de 40G/100GbE	20	Nó 20 de 40G/100GbE
21	Nó 21 de 40G/100GbE	21	Nó 21 de 40G/100GbE
22	Nó 22 de 40G/100GbE	22	Nó 22 de 40G/100GbE
23	Nó 23 de 40G/100GbE	23	Nó 23 de 40G/100GbE
24	Nó 24 de 40G/100GbE	24	Nó 24 de 40G/100GbE
25 a 30	Reservado	25 a 30	Reservado
31	ISL de 100GbE para a porta 31 do switch B	31	ISL de 100GbE para switch A porta 31
32	ISL de 100GbE para a porta 32 do switch B	32	ISL de 100GbE para switch A porta 32

Folha de exercícios de cabeamento em branco

Você pode usar a planilha de cabeamento em branco para documentar as plataformas que são suportadas como nós em um cluster. A seção *Conexões de cluster suportadas* do "[Hardware Universe](#)" Define as portas do cluster utilizadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós/portas	Porta de comutação	Utilização de nós/portas
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Chave seletora de cluster A		Chave seletora de cluster B	
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	Reservado	25 a 30	Reservado
31	ISL de 100GbE para a porta 31 do switch B	31	ISL de 100GbE para switch A porta 31
32	ISL de 100GbE para a porta 32 do switch B	32	ISL de 100GbE para switch A porta 32

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você pode ["instalar o interruptor"](#).

Instalar o switch de cluster 3232C

Siga este procedimento para instalar e configurar o switch Cisco Nexus 3232C.

Antes de começar

Certifique-se de ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#) .
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) . Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco . Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando o...	Então...
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 3232C e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 3223C em um gabinete NetApp"](#). Caso contrário, acesse ["revisar cabeamento e configuração"](#).

Instalar um switch de cluster Cisco Nexus 3232C em um gabinete NetApp

Dependendo da sua configuração, pode ser necessário instalar o switch de cluster Cisco Nexus 3232C 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 em ["Guia de Instalação de Hardware da Série Cisco Nexus 3000"](#) .

- Para cada interruptor, são necessários oito parafusos 10-32 ou 12-24 e porcas de fixação para montar os suportes e trilhos deslizantes nos postes dianteiro e traseiro do gabinete.
- Kit de trilhos padrão da Cisco para instalar o switch em um gabinete NetApp .



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Passos

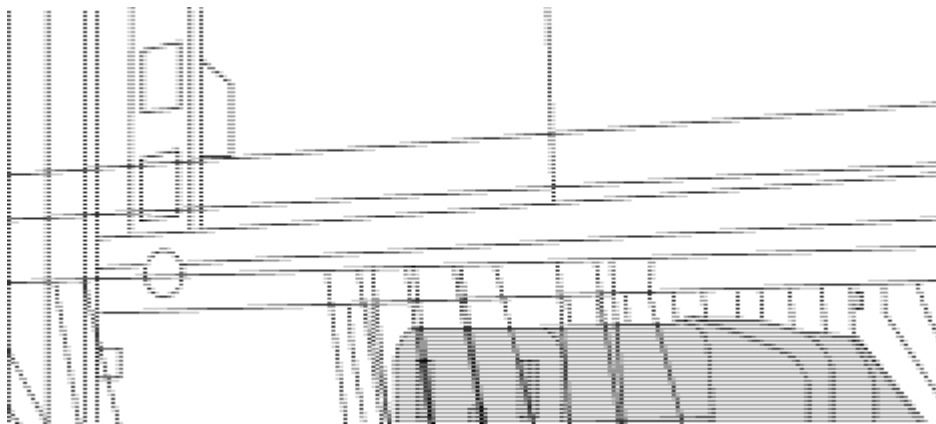
1. Instale o painel de vedação de passagem no gabinete NetApp .

O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

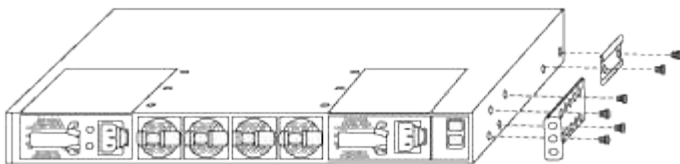
- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
 - i. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - ii. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - iii. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - iv. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.

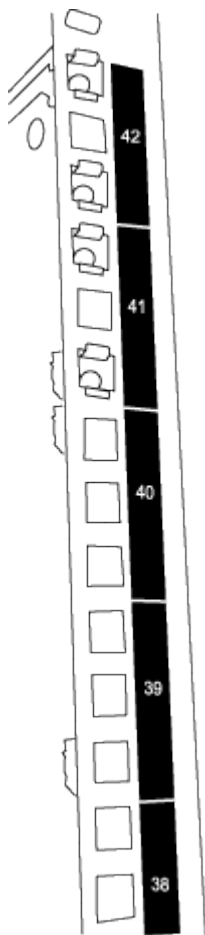


(1) Conector fêmea do cabo jumper.

1. Instale os suportes de montagem em rack no chassi do switch Nexus 3232C.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.

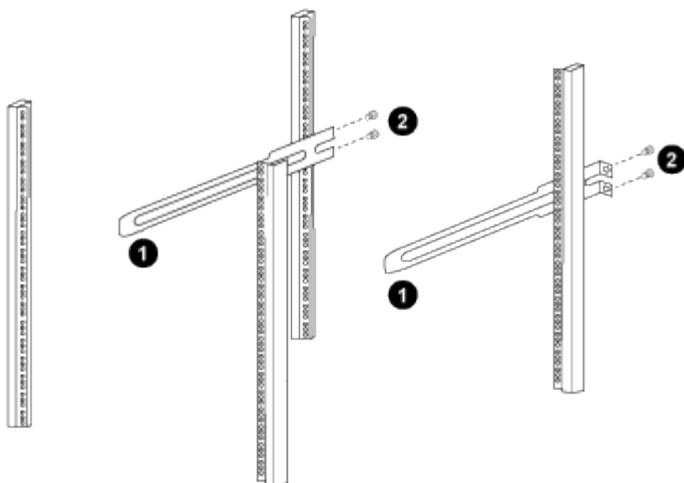


- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
2. Instale as porcas de clipe nos locais dos furos quadrados para todos os quatro postes IEA.



Os dois switches 3232C sempre serão montados no 2U superior do gabinete RU41 e 42.

3. Instale os trilhos deslizantes no armário.
 - a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os 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.

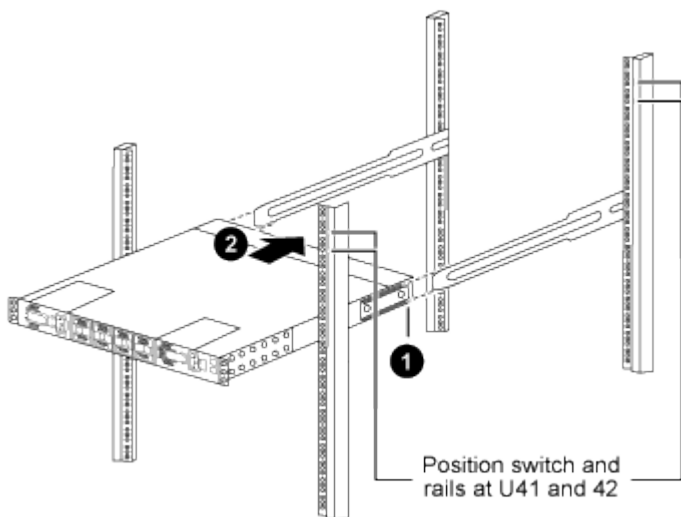
- a. Repita o passo 4a para o poste traseiro do lado direito.
- b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

4. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

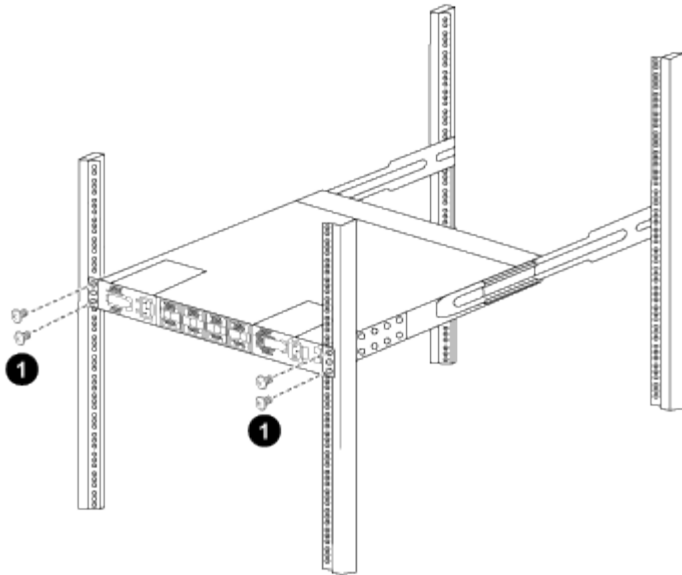
- a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

- b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

- a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos postes.
- b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

5. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
6. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

7. Conecte a porta de gerenciamento em cada switch 3232C 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seu switch Cisco 3232C, revise as seguintes considerações.

Suporte para portas Ethernet NVIDIA CX6, CX6-DX e CX7.

Ao conectar uma porta de switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir a velocidade da porta do switch manualmente.

```
(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
```

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Configurar 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 interruptor"

Configure 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 após configurar o switch Cisco 3232C pela primeira vez.

5

"Verifique a configuração SSH"

Verifique se o SSH está habilitado nos switches para usar o Ethernet Switch Health Monitor (CSHM) e os recursos de coleta de logs.

Configurar o switch de cluster 3232C

Siga este procedimento para instalar e configurar o switch Cisco Nexus 3232C.

Antes de começar

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do arquivo de configuração de referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#).
- Documentação necessária sobre a rede do cluster e os switches da rede de gerenciamento.

Consulte ["Documentação necessária"](#) para mais informações.

- Documentação do controlador e documentação do ONTAP necessárias.

["Documentação da NetApp"](#)

- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Planilhas de cabeamento concluídas.
- Arquivos RCF aplicáveis de rede de cluster NetApp e de rede de gerenciamento, baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) para os switches que você receber. Todos os switches de rede de cluster e de rede de gerenciamento da Cisco chegam com a configuração padrão de fábrica da Cisco. Esses switches também possuem a versão atual do software NX-OS, mas não têm os RCFs carregados.

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando seu...	Então...
Cisco Nexus 3232C em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 3232C e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.
4. Realize uma configuração inicial dos switches de rede do cluster.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador.	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	O nome do interruptor está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.

Incitar	Resposta
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira o número de bits da chave entre 1024 e 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.
Configurar a camada de interface padrão (L3/L2):	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado):	Responda com noshut . O padrão é noshut.
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso):	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

- Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
- Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software compatível com a NetApp para os switches a partir do ["Download do software Cisco"](#) página.

O que vem a seguir?

Depois de configurar seus switches, você pode ["Prepare-se para instalar o NX-OS e o RCF"](#).

Prepare-se para instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF).

Antes de instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam dois nós. Esses nós utilizam duas portas de interconexão de cluster de 10GbE. e0a e e0b .

Consulte o ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Nomenclatura de interruptores e nós

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2` .
- Os nomes dos nós são `cluster1-01` e `cluster1-02` .
- Os nomes 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::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

1. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do 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 do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(***>**) aparece.

3. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 do 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

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

Node: cluster1-01

Port	IPspace	Broadcast Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health 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
```

Current Vserver Port	Logical Current Is Interface Home	Status Admin/Oper	Network Address/Mask	Node

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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	Date	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		

Todas as versões do ONTAP

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

```
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. **[[passo 6]]**Verifique se o auto-revert O comando está habilitado 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

```

Vserver	Logical 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 vem a seguir?

Após preparar a instalação do software NX-OS e do RCF, você pode ["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.

Requisitos de revisão

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 da Cisco"](#). Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do NX-OS.
- ["Switches Cisco Nexus série 3000"](#). 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 dos switches Cisco .

Instale o software

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Certifique-se de concluir o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) Em seguida, siga os passos abaixo.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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

Health	Health				Speed (Mbps)	
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 principal:

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

Mostrar exemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 do software NX-OS em execução:

```
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 do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

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 após a reinicialização do switch:

```
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	Up-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 você estiver atualizando para a versão 9.3(11) do NX-OS, você deve atualizar o EPLD. golden Crie a imagem e reinicie o switch mais uma vez. Caso contrário, passe para a etapa 12.

Consulte "[Notas de versão da atualização EPLD, versão 9.3\(11\)](#)" 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 do cluster.

a. Verifique se as portas do cluster estão ativas e funcionando corretamente em todos os nós do cluster:

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

Mostrar exemplo

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

```
Node: cluster1-01
```

```
Ignore
```

Health	Health				Speed (Mbps)	
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
```

Health	Health				Speed (Mbps)	
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
```

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

b. Verifique o estado de saúde do switch no cluster.

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Model	Type	Address	
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 poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.

```

14. Verifique se o cluster está íntegro:

```
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 interruptor cs1.

16. Ative a reversão automática nos LIFs do cluster.

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

17. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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 alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que vem a seguir?

Após instalar o software NX-OS, você pode ["instalar ou atualizar o arquivo de configuração de referência \(RCF\)"](#).

Instale ou atualize o RCF

Visão geral da instalação ou atualização do Arquivo de Configuração de Referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches Nexus 3232C pela primeira vez. Você atualiza sua versão RCF quando tem uma versão existente do arquivo RCF instalada no seu switch.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configurações RCF disponíveis

A tabela a seguir descreve os RCFs disponíveis para diferentes configurações. Selecione o RCF aplicável à sua configuração.

Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

Nome da RCF	Descrição
2-Cluster-HA-Breakout	Suporta dois clusters ONTAP com pelo menos oito nós, incluindo nós que usam portas Cluster+HA compartilhadas.
4-Cluster-HA-Breakout	Suporta quatro clusters ONTAP com pelo menos quatro nós, incluindo nós que usam portas Cluster+HA compartilhadas.
1-Cluster-HA	Todas as portas estão configuradas para 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas. Requerido para os sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
1-Cluster-HA-Breakout	As portas estão configuradas para breakout 4x10GbE, breakout 4x25GbE (RCF 1.6+ em switches 100GbE) e 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas para nós que utilizam portas compartilhadas de cluster/HA: sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
Armazenamento de alta disponibilidade em cluster	As portas estão configuradas para 40/100GbE para Cluster+HA, 4x10GbE breakout para Cluster e 4x25GbE breakout para Cluster+HA, e 100GbE para cada par de armazenamento HA.
Conjunto	Duas versões do RCF com diferentes alocações de portas 4x10GbE (breakout) e portas 40/100GbE. Todos os nós FAS/ AFF são suportados, exceto os sistemas AFF A320, AFF A250 e FAS500f .
Armazenar	Todas as portas estão configuradas para conexões de armazenamento NVMe de 100GbE.

RCFs disponíveis

A tabela a seguir lista os RCFs disponíveis para switches 3232C. Escolha a versão do RCF aplicável à sua configuração. Consulte ["Switches Ethernet da Cisco"](#) para obter mais informações.

Nome da RCF
Cluster-HA-Breakout RCF v1.xx
Cluster-HA RCF v1.xx
Armazenamento RCF v1.xx
Cluster RCF 1.xx

Documentação sugerida

- ["Switches Ethernet Cisco \(NSS\)"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 3000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF dos clusters 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.

Os exemplos neste procedimento utilizam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE, **e0a** e **e0b**. Consulte a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Para obter detalhes sobre as configurações RCF disponíveis, consulte ["fluxo de trabalho de instalação de software"](#).

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

O que vem a seguir?

Após revisar a visão geral do procedimento de instalação ou atualização do RCF, você pode ["instalar o RCF"](#) ou ["atualize seu RCF"](#) Conforme necessário.

Instale o arquivo de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches Nexus 3232C pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual.
- É necessária uma conexão de console com o switch durante a instalação do RCF.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para habilitar operações de cluster sem interrupções, o procedimento a seguir migra todos os LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Certifique-se de concluir o procedimento em ["Prepare-se para instalar o NX-OS e o RCF."](#) Em seguida, siga os passos abaixo.

Passo 1: Instale o RCF nos interruptores

1. Faça login no switch cs2 usando SSH ou usando um console serial.
2. Copie o RCF para a bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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)...
```

3. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Guia de](#)

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
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

4. Examine a saída do banner 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.
5. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

6. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte ["Análise as considerações sobre cabeamento e configuração."](#) Para obter detalhes sobre quaisquer alterações adicionais necessárias.
7. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte: * Nome de usuário e senha * Endereço IP de gerenciamento * Gateway padrão * Nome do switch

```
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
```

8. Ao instalar o 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
```

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

9. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

10. Emita 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
```

11. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

12. Reinicializar switch cs2:

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

13. Repita os passos 1 a 12 no switch cs1.

14. Conecte as portas de cluster de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Etapas 2: Verifique as conexões do switch

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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 algum LIFS de cluster não tiver retornado às suas portas iniciais, reverta-o manualmente:

```
network interface revert -vserver <vserver_name> -lif <lif_name>
```

4. Verifique se o cluster está íntegro:

```
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::*>
```

Etapa 3: configurar seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e instalação de cluster, incluindo atribuição de um endereço IP de gerenciamento de nó, inicialização do cluster, criação de uma camada local, configuração de protocolos e provisionamento de armazenamento inicial.

Consulte ["Configurar o ONTAP em um novo cluster com o System Manager"](#) para obter instruções de configuração.

O que vem a seguir?

Após instalar o RCF, você pode ["verificar a configuração SSH"](#).

Atualize seu Arquivo de Configuração de Referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapas 1: Prepare-se para a atualização

1. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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 principal:

```
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: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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
```

Etapa 2: Configurar portas

1. No switch de cluster cs2, desligue as portas conectadas 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
```



Certifique-se de desligar **todas** as portas do cluster conectadas para evitar problemas de conexão de rede. Consulte o artigo da Knowledge Base ["Nó fora do quorum durante a migração do LIF do cluster na atualização do sistema operacional."](#) para obter mais detalhes.

2. Verifique se as portas do cluster falharam nas 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 íntegro:

```
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. Caso ainda não o tenha feito, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

```
show running-config
```

5. Registre quaisquer adições personalizadas entre o atual `running-config` e o arquivo RCF em uso (como uma configuração SNMP para sua organização).
6. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Certifique-se de configurar o seguinte: * Nome de usuário e senha * Endereço IP de gerenciamento * Gateway padrão * Nome do switch

```
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
```

7. Ao atualizar para a versão 1.12 ou posterior do RCF, 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
```

8. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

9. Emita 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**

10. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Reinicie o switch cs2:

```
cs2# reload
```

This command will reboot the system. (y/n)? [n] **y**

12. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

13. Copie o RCF para a bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

Mostrar exemplo

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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)...
```

14. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

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
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

15. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

16. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração](#)." Para obter detalhes sobre quaisquer alterações adicionais necessárias.
17. Após 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 os comandos da Cisco, consulte o guia apropriado na "[Guia de Comandos do Cisco Nexus Série 3000 NX-OS](#)".

```
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

18. Reinicie o switch cs2. Você pode ignorar os eventos "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs2# reload  
This command will reboot the system. (y/n)? [n] y
```

19. Verifique a integridade das portas do 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 o estado de saúde do switch no cluster (isso pode não mostrar o switch cs2, já que as LIFs não estão configuradas 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: FOXXXXXXXXGD
    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: FOXXXXXXXXGS
```

```
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 carregada anteriormente no switch 2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT: Desbloqueando a porta port-channel1 na VLAN0092. Consistência da porta restaurada. 17 de nov de 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Bloqueando port-channel1 na VLAN0001. VLAN peer inconsistente. 17 de nov de 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Bloqueando port-channel1 na VLAN0092. VLAN local inconsistente.



Pode levar até 5 minutos para que os nós do cluster sejam considerados íntegros.

20. No switch de cluster cs1, desligue as portas conectadas às portas de cluster dos nós.

Mostrar exemplo

O exemplo a seguir utiliza a saída de exemplo da interface da etapa 1:

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

21. Verifique se as LIFs do cluster foram migradas 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::*>				

22. Verifique se o cluster está íntegro:

```
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::*>
```

23. Repita os passos 4 a 19 no switch cs1.

24. Ative a reversão automática nos LIFs do cluster.

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

Etapa 3: Verifique a configuração de rede do cluster e a integridade do cluster.

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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 algum LIFS de cluster não tiver retornado às suas portas iniciais, reverta-o manualmente:

```
network interface revert -vserver vservice_name -lif lif_name
```

4. Verifique se o cluster está íntegro:

```
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::*>
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` comando para iniciar uma verificação de acessibilidade para conectividade do cluster e então exibir os detalhes:

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

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

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

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

Packet	Source	Destination	
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			
.			
.			
.			
.			

Todas as versões do ONTAP

Para todas as versões do ONTAP , você também pode usar o

cluster ping-cluster -node <name> comando para verificar a conectividade:
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 vem a seguir?

Após atualizar seu RCF, você pode ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches do 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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer           1          enabled
(switch)#
```



Ao habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Consulte ["Configure a segurança de rede usando FIPS."](#) para mais detalhes.

O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar 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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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.

O que vem a seguir

Após reiniciar o interruptor, você pode ["reconfigurar"](#) de acordo com suas necessidades.

Migrar switches

Migrar de clusters sem switches de dois nós

Migrar de um fluxo de trabalho de cluster sem switch de dois nós

Siga estes passos do fluxo de trabalho para migrar de um cluster sem switches de dois nós para um cluster com switches Cisco Nexus 3232C.



"Requisitos de migração"

Analise as informações de exemplo do switch para o processo de migração.

2

"Prepare-se para a migração"

Prepare seu cluster de dois nós sem switch para migração para um cluster de dois nós com switch.

3

"Configure suas portas"

Configure seu cluster de dois nós sem switch para migração para um cluster de dois nós com switch.

4

"Conclua sua migração"

Conclua sua migração para um cluster comutado de dois nós.

Requisitos de migração

Se você possui um cluster sem switches de dois nós, pode migrar para um cluster com switches de dois nós que inclua switches de rede de cluster Cisco Nexus 3232C. Este é um procedimento não disruptivo.

Antes de começar

Verifique as seguintes instalações e conexões:

- As portas estão disponíveis para conexões de nós. Os switches do cluster utilizam as portas Inter-Switch Link (ISL) e1/31-32.
- Você possui os cabos adequados para conexões em cluster:
 - Os nós com conexões de cluster de 10 GbE requerem módulos ópticos QSFP com cabos de fibra óptica breakout ou cabos breakout de cobre QSFP para SFP+.
 - Os nós com conexões de cluster 40/100 GbE requerem módulos ópticos QSFP/QSFP28 compatíveis com cabos de fibra óptica ou cabos de cobre QSFP/QSFP28 de conexão direta.
 - Os switches de cluster requerem a cablagem ISL apropriada:
 - 2 cabos de fibra óptica ou cobre QSFP28 com conexão direta.
- As configurações estão devidamente definidas e funcionando.

Os dois nós devem estar conectados e funcionando em um cluster sem switch de dois nós.

- Todas as portas do cluster estão no estado **ativo**.
- Os switches de cluster Cisco Nexus 3232C são suportados.
- A configuração de rede do cluster existente apresenta as seguintes características:
 - Uma infraestrutura de cluster Nexus 3232C redundante e totalmente funcional em ambos os switches.
 - As versões mais recentes do RCF e do NX-OS em seus switches.
 - Conectividade de gerenciamento em ambos os switches
 - Acesso ao console de ambos os switches
 - Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo**, sem terem sido migradas.
 - Personalização inicial do interruptor
 - Todas as portas ISL habilitadas e cabeadas

Sobre os exemplos utilizados

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Chaves 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 40 GbE **e4a** e **e4e**. O ["Hardware Universe"](#) Contém detalhes sobre as portas do cluster em suas plataformas.

- **n1_clus1** é a primeira interface lógica de cluster (LIF) a ser conectada ao switch de cluster **C1** para o nó **n1**.
- **n1_clus2** é a primeira LIF de cluster a ser conectada ao switch de cluster **C2** para o nó **n1**.
- **n2_clus1** é a primeira LIF de cluster a ser conectada ao switch de cluster **C1** para o nó **n2**.
- **n2_clus2** é a segunda LIF de cluster a ser conectada 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 no ["Download do arquivo de configuração de referência do switch de rede de cluster Cisco"](#) página.



O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

O que vem a seguir?

Após analisar os requisitos de migração, você pode ["Prepare-se para migrar seus switches."](#)

Prepare-se para a migração de clusters de dois nós sem switches para clusters de dois nós com switches.

Siga estes passos para preparar seu cluster de dois nós sem switches para migrar para um cluster de dois nós com switches que inclua switches de rede de cluster Cisco Nexus 3232C.

Passos

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período 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 respectivos nós 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
e4a      n1_clus1    up/up      10.10.0.1/24  n1
true
e4e      n1_clus2    up/up      10.10.0.2/24  n1
true
e4a      n2_clus1    up/up      10.10.0.3/24  n2
true
e4e      n2_clus2    up/up      10.10.0.4/24  n2
true

4 entries were displayed.
```

- c. Verifique se a detecção de cluster sem switch está habilitada usando o comando de privilégio avançado:

```
network options detect-switchless-cluster show`
```

Mostrar exemplo

O resultado no exemplo a seguir mostra que a detecção de clusters sem switch está habilitada:

```
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 no site, como adicionar usuários, senhas e endereços de rede.

Você deve preparar ambos os interruptores neste momento. Se precisar atualizar o RCF e o software de imagem, siga estes passos:

- a. Acesse a página *Cisco Ethernet Switches* no site de suporte da NetApp .

["Switches Ethernet da Cisco"](#)

- b. Anote o modelo do seu switch e as versões de software necessárias na tabela dessa 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.

["Download do arquivo de configuração de referência do switch de rede de gerenciamento e cluster da Cisco"](#)

- 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 voltadas para o nó C1 e C2, mas não desative as portas ISL e1/31-32.

Para obter mais informações sobre os comandos da Cisco, consulte a seguinte lista no ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 sendo desativadas nos switches C1 e C2 do cluster Nexus 3232C usando uma configuração compatível com o 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. Conecte as portas 1/31 e 1/32 em C1 às mesmas portas em C2 usando cabos compatíveis.
- 7. Verifique se as portas ISL estão operacionais em C1 e C2:

```
show port-channel summary
```

Para obter mais informações sobre os comandos da Cisco, consulte a seguinte lista no ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Mostrar exemplo

O exemplo a seguir mostra o Cisco `show port-channel summary`. O comando está sendo usado para verificar se as portas ISL estão operacionais em C1 e 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. Exibir a lista de dispositivos vizinhos no switch.

Para obter mais informações sobre os comandos da Cisco, consulte a seguinte lista no ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Mostrar exemplo

O exemplo a seguir mostra o comando `Cisco .show cdp neighbors` 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. Exibir a conectividade da porta do cluster em cada nó:

```
network device-discovery show
```


Mostrar exemplo

O exemplo a seguir mostra a conectividade 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 vem a seguir?

Depois de se preparar para migrar seus switches, você pode ["configure suas portas"](#) .

Configure suas portas para migração de um cluster sem switch de dois nós para um cluster com switch de dois nós.

Siga estes passos para configurar suas portas para migração de um cluster sem switches de dois nós para um cluster com switches 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 vservice-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, conforme 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 foram migradas com sucesso:

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

Mostrar exemplo

O exemplo a seguir mostra que o status "Is Home" para as LIFs n1_clus1 e n2_clus1 tornou-se "false" após a conclusão da migração:

```
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. Desative 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, conforme 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet			Source	Destination
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				

Todas as versões do ONTAP

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

```
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. [[passo 5]] Desconecte o cabo de e4a no nó n1.

Você pode consultar a configuração em execução e conectar a primeira porta 40 GbE do switch C1 (porta 1/7 neste exemplo) à porta e4a do switch n1 usando cabos compatíveis com switches Nexus 3232C.

2. Desconecte o cabo do e4a no nó n2.

Você pode consultar a configuração em execução e conectar o e4a à próxima porta 40 GbE disponível em C1, porta 1/8, usando cabos compatíveis.

3. Habilite todas as portas voltadas para o nó em C1.

Para obter mais informações sobre os comandos da Cisco, consulte os guias listados em "[Referências de comandos do Cisco Nexus série 3000 NX-OS](#)".

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 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 do 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 original individualmente, conforme 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 todas as LIFs foram revertidas para suas portas de origem:

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

O Is Home A coluna deve exibir um valor de true para todos os portos listados no 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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a n1_clus1 up/up 10.10.0.1/24 n1
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. Exibir a conectividade 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 o 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 de origem individualmente, conforme 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. Desative as portas do cluster clus2 LIF em ambos os nós:

```
network port modify
```

Mostrar exemplo

O exemplo a seguir mostra as portas especificadas sendo configuradas para `false`, desativando 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 do 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. Desconecte o cabo do e4e no nó n1.

Você pode consultar a configuração em execução e conectar a primeira porta 40 GbE no switch C2 (porta 1/7 neste exemplo) à porta e4e no nó n1, usando o cabeamento apropriado para o modelo de switch Nexus 3232C.

13. Desconecte o cabo do e4e no nó n2.

Você pode consultar a configuração em execução e conectar o e4e à próxima porta 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 o nó no C2.

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 sendo habilitadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração compatível com o 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 do cluster, e4e, sendo ativada 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 as LIFs migradas sendo revertidas para suas portas de origem.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

O que vem a seguir?

Depois de configurar as portas, você pode ["Conclua sua migração"](#) .

Conclua sua migração de um cluster de dois nós sem switch para um cluster de dois nós com switch.

Conclua os seguintes passos para finalizar a migração de um cluster sem switches de dois nós para um cluster com switches de dois nós em switches Nexus 3232C.

Passos

- 1. Verifique se todas as portas de interconexão do cluster foram revertidas para suas portas originais:

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

O Is Home A coluna deve exibir um valor de true para todos os portos listados no 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 do cluster estão configuradas corretamente. up estado:

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

- 3. Exibir os números das portas do switch de cluster através das quais cada porta do cluster está conectada 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 os switches de 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 detecção de cluster sem switch alterou a opção de cluster sem switch para desativada:

```
network options switchless-cluster show
```

6. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. [[passo 7]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

O que vem a seguir?

Após concluir a migração do seu switch, você poderá "[configurar monitoramento de integridade do switch](#)".

Substitua os interruptores

Substitua um switch de cluster Cisco Nexus 3232C

Siga estes passos para substituir um switch Cisco Nexus 3232C defeituoso em um cluster. Este é um procedimento não disruptivo.

Requisitos de revisão

O que você vai precisar

Certifique-se de que o cluster existente e a configuração de rede possuam as seguintes características:

- A infraestrutura do cluster Nexus 3232C é redundante e totalmente funcional em ambos os switches.

A página de switches Ethernet da Cisco contém as versões mais recentes do RCF e do NX-OS para seus switches.

- Todas as portas do cluster devem estar no estado **ativo**.
- A conectividade de gerenciamento deve existir em ambos os switches.
- Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e não foram migradas.

O switch Cisco Nexus 3232C de substituição possui as seguintes características:

- A conectividade da rede de gerenciamento está funcional.
- O acesso ao console para o interruptor de substituição já está instalado.
- A imagem apropriada do sistema operacional RCF e NX-OS é carregada no switch.
- A personalização inicial do interruptor está concluída.

Para maiores informações

Consulte o seguinte:

- ["Switches Ethernet da Cisco"](#)
- ["Hardware Universe"](#)
- ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#)

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Sobre esta tarefa

Este procedimento de substituição descreve o seguinte cenário:

- Inicialmente, o cluster possui quatro nós conectados a dois switches de cluster Nexus 3232C, CL1 e CL2.
- Você planeja substituir o switch de cluster CL2 pelo C2 (etapas 1 a 21):
 - Em cada nó, você migra as LIFs do cluster conectadas ao switch de cluster CL2 para as portas do cluster conectadas ao switch de cluster CL1.
 - Desconecte os cabos de todas as portas do switch de cluster CL2 e reconecte-os às mesmas portas no switch de cluster de substituição C2.
 - Você reverte as LIFs (Funções de Interface de Cluster) migradas em cada nó.

Sobre os exemplos

Este procedimento de substituição substitui o segundo interruptor de cluster Nexus 3232C CL2 pelo novo interruptor 3232C C2.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os quatro nós são n1, n2, n3 e n4.
- n1_clus1 é a primeira interface lógica de cluster (LIF) conectada ao switch de cluster C1 para o nó n1.
- n1_clus2 é a primeira LIF de cluster conectada ao switch de cluster CL2 ou C2 para o nó n1.
- n1_clus3 é a segunda LIF conectada ao switch de cluster C2 para o nó n1.
- n1_clus4 é a segunda LIF conectada ao switch de cluster CL1, para o nó n1.

O número de portas 10 GbE e 40/100 GbE está definido nos arquivos de configuração de referência (RCFs) disponíveis em ["Download do arquivo de configuração de referência do switch de rede de cluster Cisco"](#).

Os exemplos neste procedimento de substituição utilizam 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 o ["Hardware Universe"](#) para verificar as portas de cluster corretas para sua plataforma.

Etapa 1: Exibir e migrar as portas do cluster para o switch

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Exibir informações sobre os dispositivos na 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
n2	e0d	CL1	Ethernet1/1/2	N3K-C3232C
	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
n3	e0c	CL2	Ethernet1/1/4	N3K-C3232C
	e0d	CL1	Ethernet1/1/4	N3K-C3232C
	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
n4	e4e	CL2	Ethernet1/7	N3K-C3232C
	/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

Health      Health      Speed (Mbps)
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 de cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo de saída a seguir exibe as trocas de cluster:

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
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 NX3232C	cluster-network	10.10.1.102
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 no site.

- a. Acesse o site de suporte da NetApp .

["meusuporte.netapp.com"](https://meusuporte.netapp.com)

- b. Acesse a página * Switches Ethernet da Cisco * e observe as versões de software necessárias na tabela.

["Switches Ethernet da Cisco"](#)

- c. Faça o download da versão apropriada do RCF.

- d. Clique em **CONTINUAR** na página **Descrição**, aceite o contrato de licença e, em seguida, acesse a página **Download**.

- e. Faça o download da versão correta do software de imagem na página **Download do arquivo de configuração de referência do switch de rede de gerenciamento e cluster Cisco**.

["Download do arquivo de configuração de referência do switch de rede de gerenciamento e cluster Cisco"](#)

5. Migre as LIFs do cluster para as portas do nó físico conectadas ao switch de substituição C2:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node
node-name -destination-node node-name -destination-port port-name
```

Mostrar exemplo

Você deve migrar todas as LIFs do 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 status das portas do cluster e suas respectivas 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
e0a          n1_clus1    up/up      10.10.0.1/24      n1
true
e0a          n1_clus2    up/up      10.10.0.2/24      n1
false
e0d          n1_clus3    up/up      10.10.0.3/24      n1
false
e0d          n1_clus4    up/up      10.10.0.4/24      n1
true
e0a          n2_clus1    up/up      10.10.0.5/24      n2
true
e0a          n2_clus2    up/up      10.10.0.6/24      n2
false
e0d          n2_clus3    up/up      10.10.0.7/24      n2
false
e0d          n2_clus4    up/up      10.10.0.8/24      n2
true
e4a          n3_clus1    up/up      10.10.0.9/24      n3
true
e4a          n3_clus2    up/up      10.10.0.10/24     n3
false
e4a          n4_clus1    up/up      10.10.0.11/24     n4
true
e4a          n4_clus2    up/up      10.10.0.12/24     n4
false
```

7. Desative as portas de interconexão do cluster que estão fisicamente conectadas 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 do cluster estão desativadas 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet			Source	Destination
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				
.				
.				

Todas as versões do ONTAP

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

```
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 2: Migrar ISLs para os switches CL1 e C2

1. Desative as portas 1/31 e 1/32 no switch de cluster CL1.

Para obter mais informações sobre os comandos da Cisco, consulte os guias listados em ["Referências de comandos do Cisco Nexus série 3000 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 conectados ao switch de cluster CL2 e reconecte-os ao switch de substituição C2 para todos os nós.
3. Remova os cabos de interligação entre switches (ISL) das portas e1/31 e e1/32 no switch de cluster CL2 e reconecte-os às mesmas portas no switch de substituição C2.
4. Ative as portas ISL 1/31 e 1/32 no switch de cluster CL1.

Para obter mais informações sobre os comandos da Cisco, consulte os guias listados em ["Referências de comandos do Cisco Nexus série 3000 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 ativos no CL1.

Para obter mais informações sobre os comandos da Cisco, consulte os guias listados em ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

As portas Eth1/31 e Eth1/32 devem indicar (P) , o que significa que as portas ISL estão ativas 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 os comandos da Cisco, consulte os guias listados em ["Referências de comandos do Cisco Nexus série 3000 NX-OS"](#).

Mostrar exemplo

As portas Eth1/31 e Eth1/32 devem indicar (P), o que significa que ambas as portas ISL estão ativas 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, ative todas as portas de interconexão do cluster conectadas 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
```

Etapa 3: Reverter todas as LIFs para as 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 individualmente todas as LIFs de interconexão do cluster, 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 do cluster foram revertidas para seus valores originais:

```
network interface show
```

Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs foram revertidas com sucesso porque as portas listadas em Current Port a coluna tem o status de true no 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 conectadas:

```
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

e4a	Cluster	Cluster		up	9000	auto/40000	-

e4e	Cluster	Cluster		up	9000	auto/40000	-

-

4. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			
.			
.			

Todas as versões do ONTAP

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

```
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)
```

Etapas 4: Verifique se todas as portas e LIFs foram migradas corretamente.

1. Exiba as informações sobre os dispositivos em sua configuração inserindo 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

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
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e4a	Cluster	Cluster		up	9000	auto/40000	-
e4e	Cluster	Cluster		up	9000	auto/40000	-

Node: n4

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	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. Exclua o interruptor de cluster substituído CL2 caso ele não tenha sido removido automaticamente:

```
system cluster-switch delete -device cluster-switch-name
```

3. Verifique se os switches de cluster apropriados estão sendo monitorados:

```
system cluster-switch show
```

Mostrar exemplo

O exemplo a seguir mostra que as chaves de cluster são monitoradas porque Is Monitored estado é true .

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
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 NX3232C	cluster-network	10.10.1.103
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 desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir o interruptor, você pode ["configurar monitoramento de integridade do switch"](#) .

Substituir switches de cluster Cisco Nexus 3232C por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

Requisitos de revisão

Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

Antes de começar

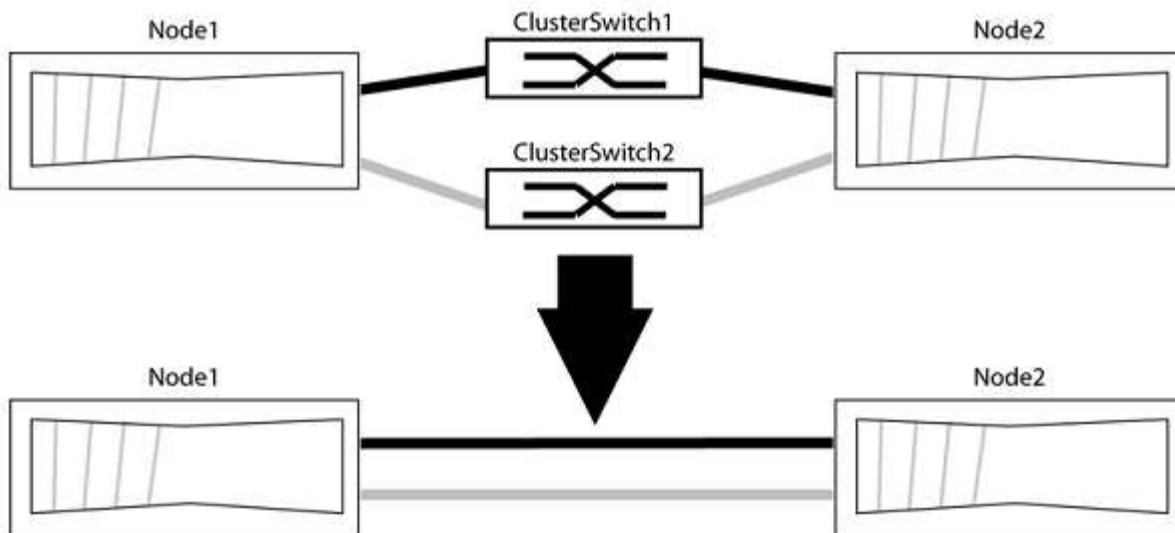
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migre 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 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 elas variam de acordo com o sistema.

Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message  
MAINT=<number_of_hours>h
```

onde *h* é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

Mostrar exemplo

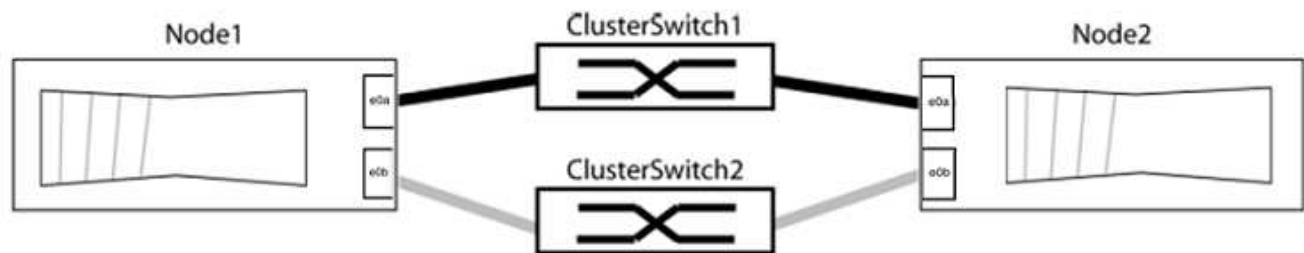
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de *up* para a coluna "Link" e um valor de *healthy* para a coluna "Estado de Saúde".

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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está `true` para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

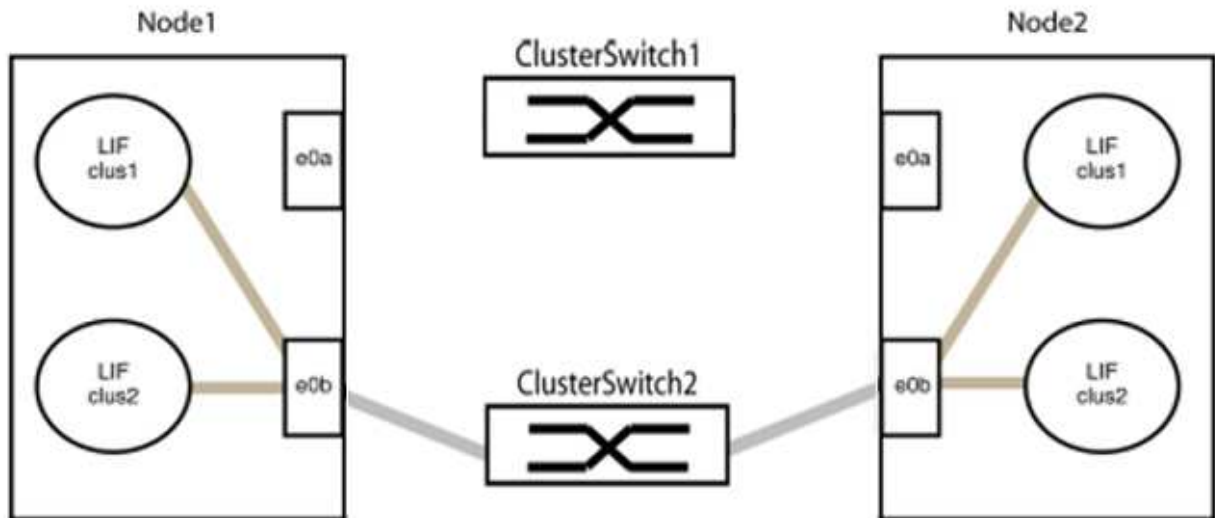
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

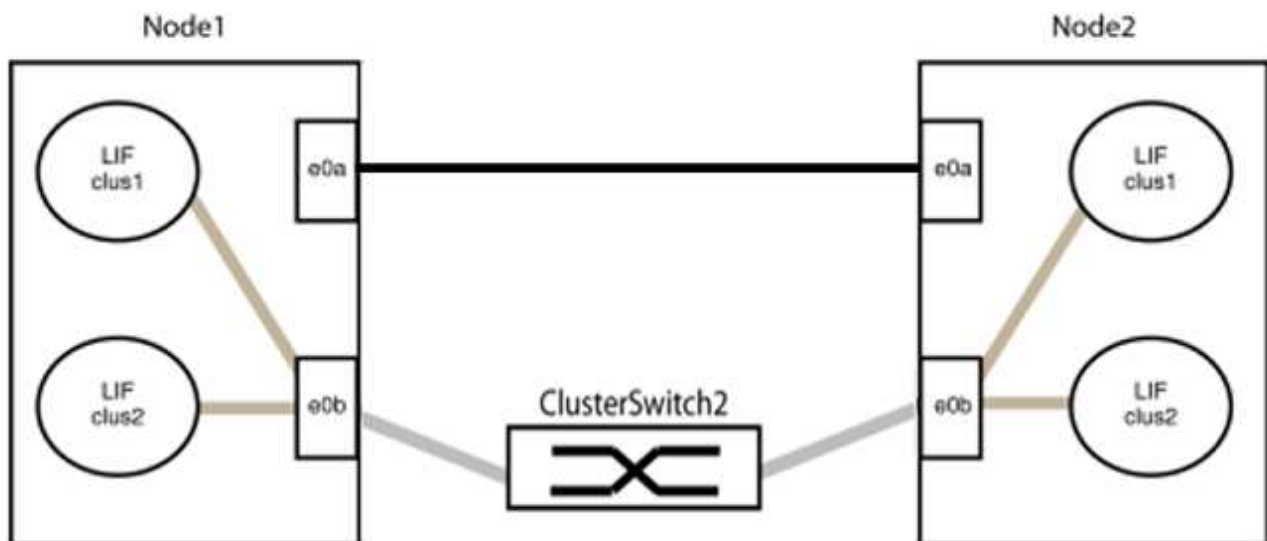
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

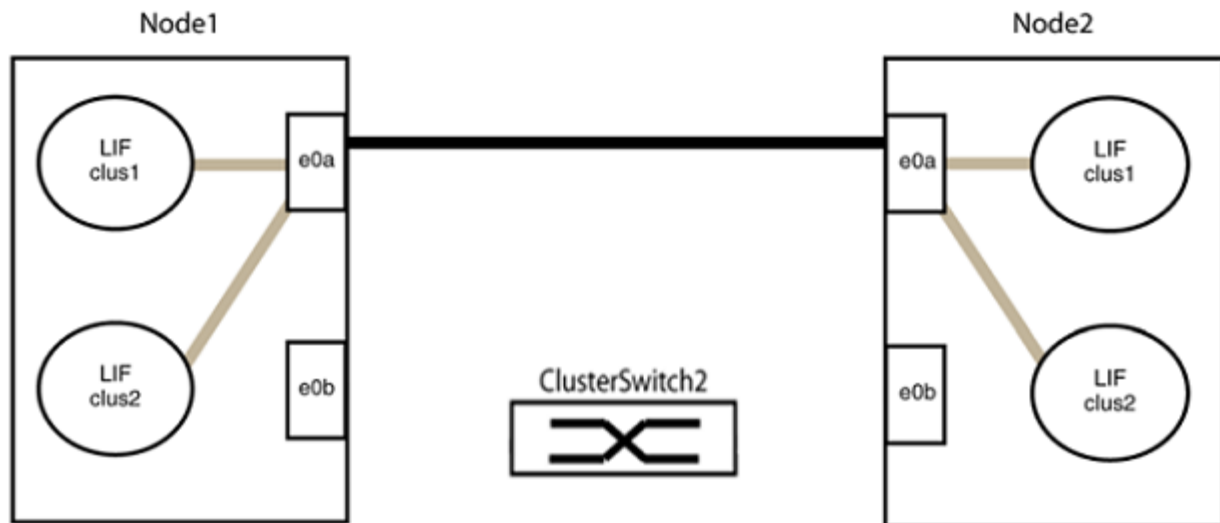
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

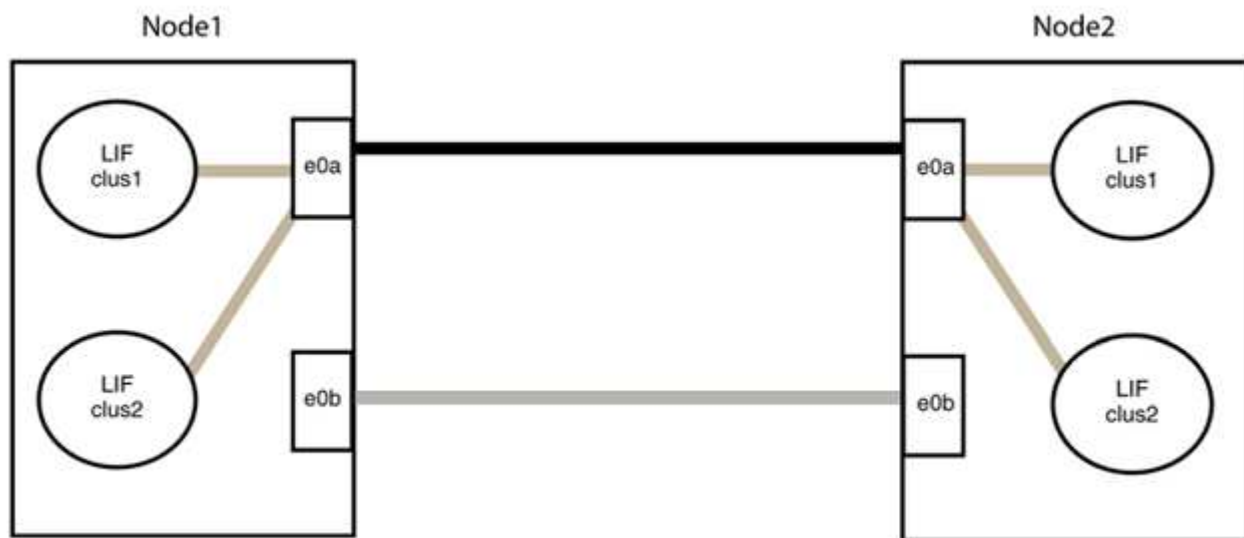
- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna "Is Home" estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todas as versões do ONTAP

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

```
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. [[passo 6]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

Cisco Nexus 3132Q-V

Começar

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 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 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 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.

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 revisar os requisitos de rede e configuração.

Requisitos de configuração

Para configurar seu cluster, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches. Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para tráfego de rede de gerenciamento.
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis.
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M, conectando-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.

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter as informações mais recentes.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

O que vem a seguir

Após analisar os requisitos de configuração, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches Cisco Nexus 3132Q-V

Para a instalação do switch Cisco Nexus 3132Q-V, certifique-se de revisar toda a documentação recomendada.

Documentação do Switch

Para configurar os switches Cisco Nexus 3132Q-V, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 3000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 3000</i>	Fornecer informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 3000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornecer as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 3000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornecer informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 3000 Series NX-OS</i>	Fornecer links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 3000</i>	Descrever os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 3000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 3000</i>	Descrever as mensagens do sistema para switches da série Cisco Nexus 3000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.

Título do documento	Descrição
Notas de versão do NX-OS para a série Cisco Nexus 3000 (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 3000.
Informações regulamentares, de conformidade e de segurança para os Cisco Nexus 6000, Cisco Nexus série 5000, Cisco Nexus série 3000 e Cisco Nexus série 2000.	Fornecer informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 3000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornecer informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco 3132Q-V em um NetApp gabinete, consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"Instalar o switch Cisco Nexus 3132Q-V em um gabinete NetApp ."	Este manual descreve como instalar um switch Cisco Nexus 3132Q-V em um gabinete NetApp de quatro postes.

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.
- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale o switch 3132Q-V.

3

"Instale o switch em um gabinete NetApp."

Instale o switch 3132Q-V e o painel de passagem em um gabinete NetApp , conforme necessário.

4

"Revisar a cablagem e a configuração."

Revise o suporte para portas Ethernet NVIDIA .

Folha de trabalho completa de cabeamento do Cisco Nexus 3132Q-V

Se você deseja documentar as plataformas suportadas, baixe o PDF desta página e preencha a planilha de cabeamento.

A planilha de cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

Cada switch pode ser configurado como uma única porta 40GbE ou como 4 portas 10GbE.

Exemplo de folha de exercícios de cabeamento

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 4x10G/40G	1	Nó 4x10G/40G
2	Nó 4x10G/40G	2	Nó 4x10G/40G
3	Nó 4x10G/40G	3	Nó 4x10G/40G
4	Nó 4x10G/40G	4	Nó 4x10G/40G
5	Nó 4x10G/40G	5	Nó 4x10G/40G
6	Nó 4x10G/40G	6	Nó 4x10G/40G
7	Nó 4x10G/40G	7	Nó 4x10G/40G
8	Nó 4x10G/40G	8	Nó 4x10G/40G
9	Nó 4x10G/40G	9	Nó 4x10G/40G
10	Nó 4x10G/40G	10	Nó 4x10G/40G
11	Nó 4x10G/40G	11	Nó 4x10G/40G
12	Nó 4x10G/40G	12	Nó 4x10G/40G
13	Nó 4x10G/40G	13	Nó 4x10G/40G
14	Nó 4x10G/40G	14	Nó 4x10G/40G
15	Nó 4x10G/40G	15	Nó 4x10G/40G
16	Nó 4x10G/40G	16	Nó 4x10G/40G
17	Nó 4x10G/40G	17	Nó 4x10G/40G

Chave seletora de cluster A		Chave seletora de cluster B	
18	Nó 4x10G/40G	18	Nó 4x10G/40G
19	Nó 19 de 40G	19	Nó 19 de 40G
20	Nó 20 de 40G	20	Nó 20 de 40G
21	Nó 21 de 40G	21	Nó 21 de 40G
22	Nó 22 de 40G	22	Nó 22 de 40G
23	Nó 23 de 40G	23	Nó 23 de 40G
24	Nó 24 de 40G	24	Nó 24 de 40G
25 a 30	Reservado	25 a 30	Reservado
31	ISL de 40G para a porta 31 do switch B	31	ISL de 40G para switch A porta 31
32	ISL de 40G para a porta 32 do switch B	32	ISL de 40G para switch A porta 32

Folha de exercícios de cabeamento em branco

Você pode usar a planilha de cabeamento em branco para documentar as plataformas suportadas como nós em um cluster. A seção *Conexões de Cluster Suportadas* do "[Hardware Universe](#)" define as portas de cluster usadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós/portas	Porta de comutação	Utilização de nós/portas
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	

Chave seletora de cluster A		Chave seletora de cluster B	
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	Reservado	25 a 30	Reservado
31	ISL de 40G para a porta 31 do switch B	31	ISL de 40G para switch A porta 31
32	ISL de 40G para a porta 32 do switch B	32	ISL de 40G para switch A porta 32

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você ["instalar o interruptor"](#).

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 ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#).
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#). Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco. Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando o...	Então...
Cisco Nexus 9336C-FX2 em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 3132Q-V e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 3132Q-V em um gabinete NetApp"](#). Caso contrário, você pode ["Analisar a cablagem e a configuração."](#) requisitos.

Instalar 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 de passagem em um gabinete NetApp com os suportes padrão que acompanham o switch.

Antes de começar

- Os requisitos de preparação inicial, o conteúdo do kit e as precauções de segurança em ["Guia de Instalação de Hardware da Série Cisco Nexus 3000"](#). Analise estes documentos antes de iniciar o procedimento.

- O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6). O kit do painel de passagem da NetApp contém o seguinte hardware:
 - Um painel de obturação de passagem
 - Quatro parafusos 10-32 x 0,75
 - Quatro porcas de clipe 10-32
- Oito parafusos 10-32 ou 12-24 e porcas de fixação para montar os suportes e trilhos deslizantes nos postes dianteiros e traseiros do gabinete.
- Kit de trilhos padrão da Cisco para instalar o switch em um gabinete NetApp .

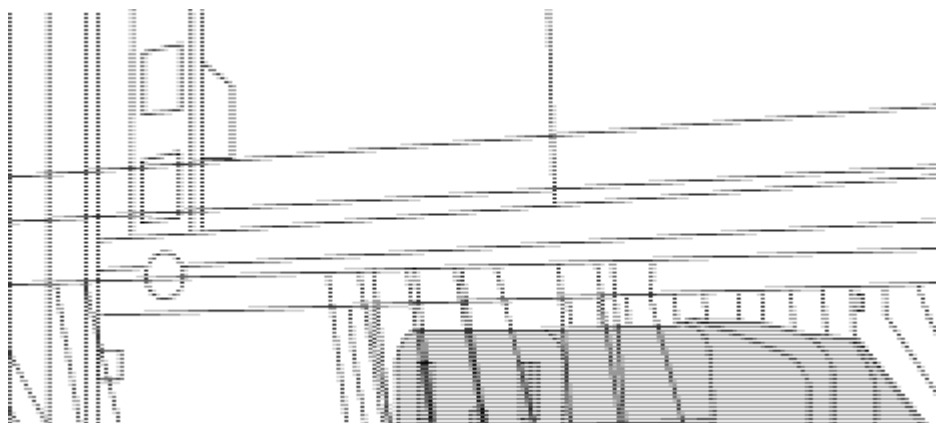


Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Passos

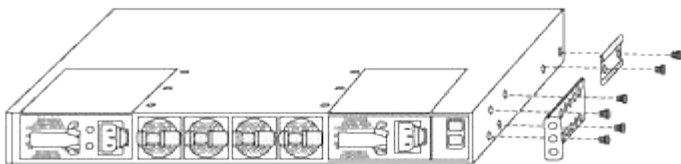
1. Instale o painel de vedação de passagem no gabinete NetApp .
 - a. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - b. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - c. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - d. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.

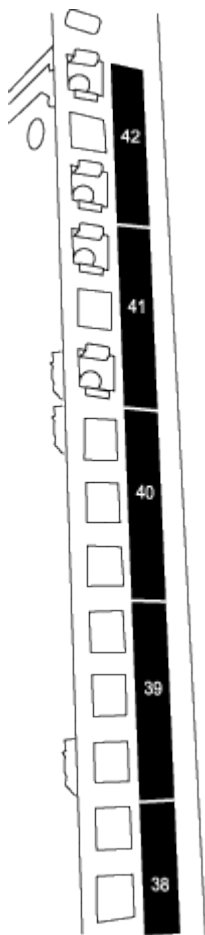


(1) Conector fêmea do cabo jumper.

2. Instale os suportes de montagem em rack no chassi do switch Nexus 3132Q-V.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.

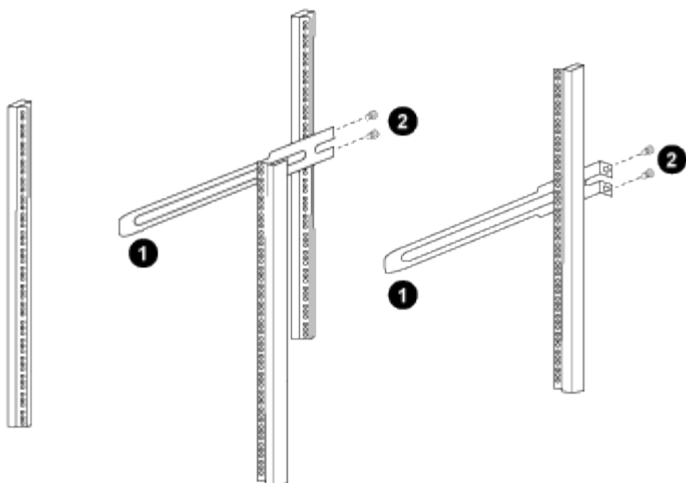


- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
3. Instale as porcas de clipe nos locais dos furos quadrados para todos os quatro postes IEA.



Os dois switches 3132Q-V sempre serão montados no 2U superior do gabinete RU41 e 42.

4. Instale os trilhos deslizantes no armário.
 - a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os com os dedos.



(1) Ao deslizar suavemente o trilho deslizante, alinhe-o com os orifícios dos parafusos na cremalheira.

(2) Aperte os parafusos dos trilhos deslizantes nos postes do gabinete.

a. Repita o passo 4a para o poste traseiro do lado direito.

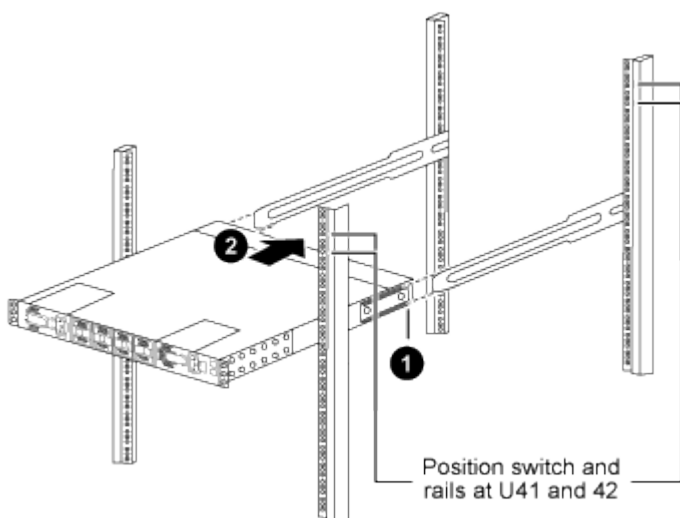
b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

5. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

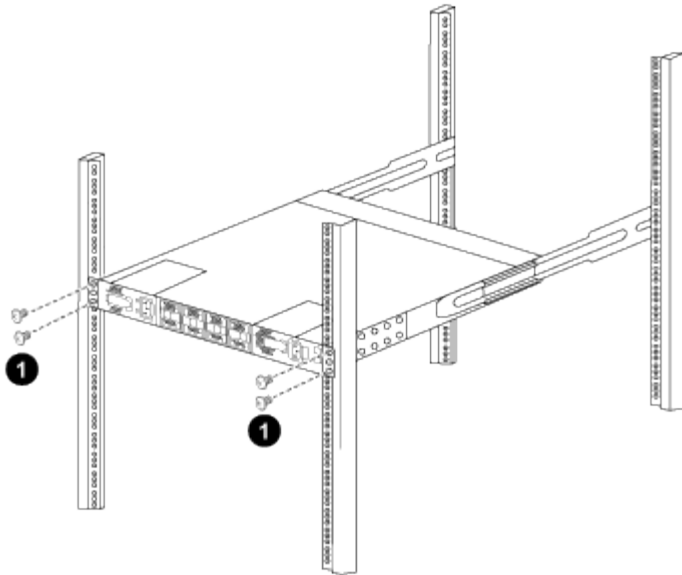
a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

- a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos postes.
- b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o interruptor já instalado como suporte, você não precisa segurar a parte frontal do segundo interruptor durante o processo de instalação.

6. Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
7. Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

8. Conecte a porta de gerenciamento em cada switch 3132Q-V 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar 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 Ethernet NVIDIA CX6, CX6-DX e CX7.

Ao conectar uma porta de switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir a velocidade da porta do switch manualmente.

```
(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 de switch. Consulte o ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

Configurar 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 interruptor"

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 ou atualize o RCF"

Instale ou atualize o RCF após configurar o switch Cisco 3132Q-V.

5

"Verifique a configuração 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 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 local de instalação para baixar as versões aplicáveis do NX-OS e do arquivo de configuração de referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#).
- Documentação necessária do switch de rede, documentação do controlador e documentação do ONTAP. Para mais informações, consulte ["Documentação necessária"](#).
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Planilhas de cabeamento preenchidas. Consulte ["Folha de trabalho completa de cabeamento do Cisco Nexus 3132Q-V"](#).
- Arquivos RCF aplicáveis de rede de cluster NetApp e de rede de gerenciamento, baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#) para os switches que você receber. Todos os switches de rede de cluster e de rede de gerenciamento da Cisco chegam com a configuração padrão de fábrica da Cisco. Esses switches também possuem a versão atual do software NX-OS, mas não têm os RCFs carregados.

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando seu...	Então...
Cisco Nexus 3132Q-V em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 3132Q-V e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando a planilha de cabeamento preenchida, conforme descrito em ["Folha de trabalho completa de cabeamento do Cisco Nexus 3132Q-V"](#).
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.
4. Realize uma configuração inicial dos switches de rede do cluster.

Ao ligar o switch pela primeira vez, responda às seguintes perguntas de configuração inicial, conforme necessário. A política de segurança do seu site define as respostas e os serviços a serem ativados.

Incitar	Resposta
Cancelar o provisionamento automático e continuar com a configuração normal? (sim/não)	Responda com sim . A opção padrão é não.
Deseja implementar um padrão de senhas seguras? (sim/não)	Responda com sim . A opção padrão é sim.
Digite a senha de administrador:	A senha padrão é "admin"; você deve criar uma nova senha forte. Uma senha fraca pode ser rejeitada.

Incitar	Resposta
Deseja acessar a caixa de diálogo de configuração básica? (sim/não)	Responda com sim na configuração inicial do switch.
Criar outra conta de login? (sim/não)	Sua resposta depende das políticas do seu site em relação a administradores alternativos. A opção padrão é não .
Configurar string de comunidade SNMP somente leitura? (sim/não)	Responda com não . A opção padrão é não.
Configurar string de comunidade SNMP de leitura e gravação? (sim/não)	Responda com não . A opção padrão é não.
Digite o nome do interruptor.	O nome do interruptor está limitado a 63 caracteres alfanuméricos.
Continuar com a configuração de gerenciamento fora de banda (mgmt0)? (sim/não)	Responda com sim (a opção padrão) quando solicitado. No prompt "mgmt0 IPv4 address:", digite seu endereço IP: ip_address.
Configurar o gateway padrão? (sim/não)	Responda com sim . No prompt "Endereço IPv4 do gateway padrão:", insira o seu gateway padrão.
Configurar opções avançadas de IP? (sim/não)	Responda com não . A opção padrão é não.
Habilitar o serviço Telnet? (sim/não)	Responda com não . A opção padrão é não.
O serviço SSH está ativado? (sim/não)	Responda com sim. A opção padrão é sim.  Recomenda-se o uso de SSH ao utilizar o Ethernet Switch Health Monitor (CSHM) devido aos seus recursos de coleta de logs. O SSHv2 também é recomendado para maior segurança.
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/rsa1).	O padrão é rsa .
Insira o número de bits da chave (1024-2048).	Insira os bits-chave de 1024 a 2048.
Configurar o servidor NTP? (sim/não)	Responda com não . A opção padrão é não.

Incitar	Resposta
Configurar a camada de interface padrão (L3/L2):	Responda com L2 . O padrão é L2.
Configurar o estado padrão da interface da porta do switch (desligado/não desligado):	Responda com noshut . O padrão é noshut.
Configurar perfil do sistema CoPP (estrito/moderado/tolerante/denso):	Responda com rigoroso . O padrão é estrito.
Deseja editar a configuração? (sim/não)	Você deverá ver a nova configuração neste ponto. Revise e faça as alterações necessárias na configuração que você acabou de inserir. Responda com não quando solicitado, caso esteja satisfeito com a configuração. Responda com sim se desejar editar suas configurações.
Usar esta configuração e salvá-la? (sim/não)	Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.  Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.

- Verifique as opções de configuração selecionadas na tela que aparece ao final da configuração e certifique-se de salvar as alterações.
- Verifique a versão nos switches de rede do cluster e, se necessário, baixe a versão do software compatível com a NetApp para os switches a partir do ["Download do software Cisco"](#) página.

O que vem a seguir?

Depois de configurar seus switches, você ["Prepare-se para instalar o NX-OS e o RCF"](#).

Prepare-se para instalar o software NX-OS e o arquivo de configuração de referência.

Antes de instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF), siga este procedimento.

Sobre os exemplos

Os exemplos neste procedimento utilizam dois nós. Esses nós utilizam duas portas de interconexão de cluster de 10GbE. e0a e e0b .

Consulte o ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `cluster1-01` e `cluster1-02`.
- Os nomes 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::*>` O prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Passos

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

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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

```
set -privilege advanced
```

O prompt avançado(`*>`) aparece.

3. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
-----	-----	-----	-----	
cluster1-02/cdp				
C3132Q-V	e0a	cs1	Eth1/2	N3K-
C3132Q-V	e0b	cs2	Eth1/2	N3K-
cluster1-01/cdp				
C3132Q-V	e0a	cs1	Eth1/1	N3K-
C3132Q-V	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

4. Verifique o status administrativo ou operacional de cada interface do 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
```

Current Is	Logical	Status	Network	Current
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o comando `show` para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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		

Todas as versões do ONTAP

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

```
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. **[[passo 6]]**Verifique se o auto-revert O comando está habilitado 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
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

O que vem a seguir?

Depois de se preparar para instalar o software NX-OS e o RCF, você "[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.

Requisitos de revisão

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 de switches para obter informações sobre as versões suportadas do ONTAP e do NX-OS.
- "[Switches Cisco Nexus série 3000](#)". 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 dos switches Cisco .

Instale o software

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Certifique-se de concluir o procedimento em "[Prepare-se para instalar o software NX-OS e o arquivo de configuração de referência](#)." Em seguida, siga os passos abaixo.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade 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. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão **ativas** e com status íntegro:

```
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

Health	Health				Speed (Mbps)	
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 principal:

```
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. As LIFs do cluster são transferidas para o switch do cluster parceiro em caso de failover 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 mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Guia de Comandos do Cisco Nexus Série 3000 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 do software NX-OS em execução:

```
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 do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

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 após a reinicialização do switch:

```
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 do cluster.

a. Verifique se as portas do cluster estão ativas e funcionando corretamente 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

Health	Health				Speed (Mbps)	
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 o estado de saúde do switch no cluster.

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

Mostrar exemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

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 Model	Type	Address	

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 poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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.

```

11. Verifique se o cluster está íntegro:

```
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 interruptor cs1.

13. Ative a reversão automática nos LIFs do cluster.

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


14. Verifique se as LIFs do cluster retornaram à sua porta original:

```
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 alguma LIF do cluster não tiver retornado às suas portas originais, reverta-as manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

O que vem a seguir?

Após instalar o software NX-OS, você pode ["instalar ou atualizar o arquivo de configuração de referência \(RCF\)"](#).

Instale ou atualize o RCF

Visão geral da instalação ou atualização do Arquivo de Configuração de Referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches Nexus 3132Q-V pela primeira vez. Você atualiza sua versão RCF quando tem uma versão existente do arquivo RCF instalada no seu switch.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Configurações RCF disponíveis

A tabela a seguir descreve os RCFs disponíveis para diferentes configurações. Selecione o RCF aplicável à sua configuração.

Para obter detalhes específicos sobre o uso de portas e VLANs, consulte a seção de avisos e notas importantes no seu RCF.

Nome da RCF	Descrição
2-Cluster-HA-Breakout	Suporta dois clusters ONTAP com pelo menos oito nós, incluindo nós que usam portas Cluster+HA compartilhadas.
4-Cluster-HA-Breakout	Suporta quatro clusters ONTAP com pelo menos quatro nós, incluindo nós que usam portas Cluster+HA compartilhadas.
1-Cluster-HA	Todas as portas estão configuradas para 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas. Requerido para os sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
1-Cluster-HA-Breakout	As portas estão configuradas para breakout 4x10GbE, breakout 4x25GbE (RCF 1.6+ em switches 100GbE) e 40/100GbE. Suporta tráfego compartilhado de cluster/HA em portas para nós que utilizam portas compartilhadas de cluster/HA: sistemas AFF A320, AFF A250 e FAS500f . Além disso, todas as portas podem ser usadas como portas dedicadas de cluster.
Armazenamento de alta disponibilidade em cluster	As portas estão configuradas para 40/100GbE para Cluster+HA, 4x10GbE breakout para Cluster e 4x25GbE breakout para Cluster+HA, e 100GbE para cada par de armazenamento HA.
Conjunto	Duas versões do RCF com diferentes alocações de portas 4x10GbE (breakout) e portas 40/100GbE. Todos os nós FAS/ AFF são suportados, exceto os sistemas AFF A320, AFF A250 e FAS500f .
Armazenar	Todas as portas estão configuradas para conexões de armazenamento NVMe de 100GbE.

RCFs disponíveis

A tabela a seguir lista os RCFs disponíveis para os switches 3132Q-V. Escolha a versão de RCF aplicável para sua configuração. Consulte ["Switches Ethernet da Cisco"](#) para mais informações.

Nome da RCF
Cluster-HA-Breakout RCF v1.xx
Cluster-HA RCF v1.xx
Cluster RCF 1.xx

Documentação sugerida

- ["Switches Ethernet Cisco \(NSS\)"](#)

Consulte a tabela de compatibilidade de switches para obter informações sobre as versões ONTAP e RCF suportadas no site de suporte da NetApp . Note que pode haver dependências entre a sintaxe de comandos no RCF e a sintaxe encontrada em versões específicas do NX-OS.

- ["Switches Cisco Nexus série 3000"](#)

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 dos switches Cisco .

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF dos clusters 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::*>` O prompt indica o nome do cluster.

Os exemplos neste procedimento utilizam quatro nós. Esses nós usam duas portas de interconexão de cluster 10GbE, **e0a** e **e0b**. Consulte a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.



Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Para obter detalhes sobre as configurações RCF disponíveis, consulte ["fluxo de trabalho de instalação de software"](#).

Comandos utilizados

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

O que vem a seguir?

Depois de revisar o procedimento de instalação do RCF ou atualização do RCF, você ["instalar o RCF"](#) ou ["atualize seu RCF"](#) conforme necessário.

Instale o arquivo de configuração de referência (RCF)

Você instala o arquivo de configuração de referência (RCF) após configurar os switches

Nexus 3132Q-V pela primeira vez.

Antes de começar

Verifique as seguintes instalações e conexões:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O RCF atual.
- É necessária uma conexão de console com o switch durante a instalação do RCF.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para habilitar operações de cluster sem interrupções, o procedimento a seguir migra todos os LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Passo 1: Instale o RCF nos interruptores

1. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
network port show -ip space 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 principal:

```
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: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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 ONTAP 9.8 e versões posteriores, 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, desligue as portas conectadas 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 do cluster falharam nas 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 íntegro:

```
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::*>
```

7. Caso ainda não o tenha feito, 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 a configuração atual e o arquivo RCF em uso.



Certifique-se de configurar o seguinte: * Nome de usuário e senha * Endereço IP de gerenciamento * Gateway padrão * Nome do switch

9. Salve os detalhes básicos de 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. Ao instalar o 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
```

Consulte ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais detalhes.

11. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

12. Emita 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 para a configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

14. Reinicie o switch:

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

15. Repita os passos 7 a 14 no switch cs1.
16. Conecte as portas de cluster de todos os nós no cluster ONTAP aos switches cs1 e cs2.

Passo 2: Verifique as conexões do interruptor

1. Verifique se as portas do switch conectadas às portas do cluster estão **ativas**.

```
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 a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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 íntegro:

```
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::*>
```

Etapa 3: configurar seu cluster ONTAP

A NetApp recomenda que você utilize o System Manager para configurar novos clusters.

O System Manager fornece um fluxo de trabalho simples e fácil para configuração e instalação de cluster, incluindo atribuição de um endereço IP de gerenciamento de nó, inicialização do cluster, criação de uma camada local, configuração de protocolos e provisionamento de armazenamento inicial.

Consulte ["Configurar o ONTAP em um novo cluster com o System Manager"](#) para obter instruções de configuração.

O que vem a seguir?

Após instalar o RCF, você pode ["verificar a configuração SSH"](#).

Atualize seu Arquivo de Configuração de Referência (RCF)

Você atualiza a versão do RCF quando já possui uma versão do arquivo RCF instalada em seus switches operacionais.

Antes de começar

Certifique-se de ter 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 a versão do seu RCF, precisará de uma configuração de inicialização no RCF que reflita as imagens de inicialização desejadas.

Se 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 reinicializações futuras.



Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.



Antes de instalar uma nova versão de software do switch e os RCFs, você deve apagar as configurações do switch e realizar a configuração básica. Você precisa estar conectado ao switch usando o console serial ou ter preservado as informações básicas de configuração antes de apagar as configurações do switch.

Etapa 1: Prepare-se para a atualização

1. Exibir as portas do cluster em cada nó que estão conectadas 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 do cluster.

a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
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

Health	Health				Speed (Mbps)	
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 principal:

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

Mostrar exemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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 ONTAP 9.8 e versões posteriores, 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.

Etapa 2: Configurar portas

1. No switch de cluster cs2, desligue as portas conectadas 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.

2. Verifique se as portas do cluster falharam nas 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::*>

```

3. Verifique se o cluster está íntegro:

```
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::*>
```

4. Caso ainda não o tenha feito, salve uma cópia da configuração atual do switch copiando a saída do seguinte comando para um arquivo de texto:

```
show running-config
```

5. Registre quaisquer adições personalizadas entre a configuração atual e o arquivo RCF em uso.

Certifique-se de configurar o seguinte:



- Nome de usuário e senha
- Endereço IP de gerenciamento
- Gateway padrão
- Nome do interruptor

6. Salve os detalhes básicos de configuração em `write_erase.cfg` arquivo no bootflash.



Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e realizar a configuração básica.

```
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
```

7. Ao atualizar para a versão 1.12 ou posterior do RCF, 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
```

8. Verifique se o `write_erase.cfg` O arquivo foi preenchido conforme o esperado:

```
show file bootflash:write_erase.cfg
```

9. Emita 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**

10. Copie a configuração básica salva anteriormente para a configuração de inicialização.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Reinicie o switch:

```
cs2# reload
```

This command will reboot the system. (y/n)? [n] **y**

12. Após o endereço IP de gerenciamento estar acessível novamente, faça login no switch via SSH.

Você pode precisar atualizar as entradas do arquivo hosts relacionadas às chaves SSH.

13. Copie o RCF para a bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

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)...
```

14. Aplique o RCF previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#).

Mostrar exemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands
```



Certifique-se de ler atentamente as seções **Notas de instalação**, **Notas importantes** e **banner** do seu RCF. Você deve ler e seguir estas instruções para garantir a configuração e operação corretas do switch.

15. Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.



Para obter instruções sobre como ativar suas portas 10GbE após uma atualização do RCF, consulte o artigo da Knowledge Base ["As portas 10GbE em um switch de cluster Cisco 3132Q não ficam online."](#).

16. Depois de verificar se as versões RCF e as configurações do switch estão corretas, copie o running-config arquivo para o startup-config arquivo.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado na ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#). .Mostrar exemplo

```
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

1. Reinicie o switch cs2. Você pode ignorar os eventos "portas do cluster inativas" relatados nos nós durante a reinicialização do switch, bem como o erro. % Invalid command at '^' marker saída.

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

2. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração.](#)" Para obter detalhes sobre quaisquer alterações adicionais necessárias.
3. Verifique a integridade das portas do cluster.
 - a. Verifique se as portas do cluster estão ativas e funcionando corretamente 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

Health	Health					Speed (Mbps)
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 o estado de saúde do switch 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
-----
-----
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: FOXXXXXXXXGD
    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: FOXXXXXXXXGS
    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 ONTAP 9.8 e versões posteriores, use o comando `system switch ethernet show -is-monitoring-enabled-operational true`.

Você poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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 do cluster sejam considerados íntegros.

4. No switch de cluster cs1, desligue as portas conectadas 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.

5. Verifique se as LIFs do cluster foram migradas 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::*>				

6. Verifique se o cluster está íntegro:

```
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. Repita os passos 1 a 19 no switch cs1.
8. Ative a reversão automática nos LIFs do cluster.

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

9. Reinicie o interruptor cs1. Você faz isso para que as LIFs do cluster voltem às suas portas originais. Você pode ignorar os eventos "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
This command will reboot the system. (y/n)? [n] y
```

Etapa 3: Verifique a configuração

1. Verifique se as portas do switch conectadas às portas do cluster estão ativas.

```
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 a ISL entre cs1 e cs2 está funcionando:

```
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 foram revertidos para 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				
	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 íntegro:

```
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o comando `show` para exibir os detalhes.

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

Packet	Source	Destination
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		

Todas as versões do ONTAP

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

```
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 vem a seguir?

Depois de atualizar seu RCF, você ["verificar a configuração SSH"](#) .

Verifique sua configuração SSH.

Se você estiver usando o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches do 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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer           1          enabled
(switch)#
```



Ao habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Consulte ["Configure a segurança de rede usando FIPS."](#) para mais detalhes.

O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar 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 precisa estar conectado ao switch usando o console serial.
- Esta tarefa redefine a configuração da rede de gerenciamento.

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.

O que vem a seguir

Após reiniciar o interruptor, você pode ["reconfigurar"](#) de acordo com suas necessidades.

Migrar switches

Migre de clusters sem switches para clusters com switches de dois nós.

Fluxo de trabalho de migração de clusters sem switches para clusters com switches de dois nós

Siga estes passos do fluxo de trabalho para migrar de um cluster sem switches de dois nós para um cluster com switches de dois nós que inclua switches de rede de cluster Cisco Nexus 3132Q-V.

1

["Requisitos de migração"](#)

Analise os requisitos e exemplos de informações de troca para o processo de migração.

2

"Prepare-se para a migração"

Prepare seus clusters sem switches para a migração para clusters com switches de dois nós.

3

"Configure suas portas"

Configure suas portas para migração de clusters de dois nós sem switch para clusters de dois nós com switch.

4

"Conclua sua migração"

Conclua sua migração de clusters sem switches para clusters com switches de dois nós.

Requisitos de migração

Se você possui um cluster sem switch de dois nós, revise este procedimento para verificar os requisitos aplicáveis para migrar para um cluster com switch de dois nós.



O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; 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

Ao migrar para um cluster comutado de dois nós com switches de cluster Cisco Nexus 3132Q-V, certifique-se de compreender as conexões de porta e de nó, bem como os requisitos de cabeamento.

- Os switches do cluster utilizam as portas Inter-Switch Link (ISL) e1/31-32.
- O ["Hardware Universe"](#) contém informações sobre a cablagem compatível com os switches Nexus 3132Q-V:
 - Os nós com conexões de cluster de 10 GbE requerem módulos ópticos QSFP com cabos de fibra óptica breakout ou cabos breakout de cobre QSFP para SFP+.
 - Os nós com conexões de cluster de 40 GbE requerem módulos ópticos QSFP/QSFP28 compatíveis com cabos de fibra óptica ou cabos de cobre QSFP/QSFP28 de conexão direta.
 - Os switches do cluster utilizam a cablagem ISL apropriada: 2 cabos de fibra óptica QSFP28 ou cabos de cobre de ligação direta.
- No Nexus 3132Q-V, você pode operar as portas QSFP nos 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 seguindo uma convenção de nomenclatura de 2 elementos. Por exemplo, a segunda porta Ethernet de 40 Gb é numerada como 1/2. O processo de alterar a configuração de Ethernet de 40 Gb para Ethernet de 10 Gb é chamado de *breakout* e o processo de alterar a configuração de Ethernet de 10 Gb

para Ethernet de 40 Gb é chamado de *breakin*. Ao dividir uma porta Ethernet de 40 Gb em portas Ethernet de 10 Gb, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 elementos. Por exemplo, as portas de conexão da segunda porta Ethernet de 40 Gb são numeradas como 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- No lado esquerdo do Nexus 3132Q-V encontra-se 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 no Nexus 3132Q-V usando o seguinte: `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 ter configurado algumas das portas do Nexus 3132Q-V para funcionar em 10 GbE ou 40 GbE.

Você pode configurar as seis primeiras portas para o modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as seis primeiras portas QSFP+ da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- O número de portas 10 GbE e 40 GbE está definido nos arquivos de configuração de referência (RCFs) disponíveis em "[Download do arquivo de configuração de referência do switch de rede de cluster Cisco](#)".

Antes de começar

- Configurações devidamente definidas e em funcionamento.
- Nós que executam o ONTAP 9.4 ou posterior.
- Todas as portas do cluster no `up` estado.
- O switch de cluster Cisco Nexus 3132Q-V é compatível.
- A configuração de rede do cluster existente possui:
 - A infraestrutura do cluster Nexus 3132 é redundante e totalmente funcional em ambos os switches.
 - As versões mais recentes do RCF e do NX-OS em seus switches.

"[Switches Ethernet da Cisco](#)" contém informações sobre as versões do ONTAP e do NX-OS suportadas neste procedimento.

- Conectividade de gerenciamento em ambos os switches.
- Acesso ao console de ambos os switches.
- Todas as interfaces lógicas de cluster (LIFs) no `up` estado sem ser migrado.
- Personalização inicial do interruptor.
- Todas as portas ISL estão habilitadas e cabeadas.

Além disso, você deve 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 utilizados

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Chaves 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 40 GbE **e4a** e **e4e**. O "[Hardware Universe](#)" Contém detalhes sobre as portas do cluster em suas plataformas.

Este procedimento abrange os seguintes cenários:

- **n1_clus1** é a primeira interface lógica de cluster (LIF) a ser conectada ao switch de cluster C1 para o nó **n1**.
- **n1_clus2** é a primeira LIF de cluster a ser conectada ao switch de cluster C2 para o nó **n1**.
- **n2_clus1** é a primeira LIF de cluster a ser conectada ao switch de cluster C1 para o nó **n2**.
- **n2_clus2** é a segunda LIF de cluster a ser conectada ao switch de cluster C2 para o nó **n2**.
- O número de portas 10 GbE e 40 GbE está definido nos arquivos de configuração de referência (RCFs) disponíveis em "[Download do arquivo de configuração de referência do switch de rede de cluster Cisco](#)".



O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 3000; os comandos ONTAP são usados, a menos que indicado de outra forma.

- O cluster inicia com dois nós conectados e funcionando em uma configuração de cluster sem switch de dois nós.
- A primeira porta do cluster foi movida para C1.
- A segunda porta do cluster foi movida para C2.
- A opção de cluster sem switch de dois nós está desativada.

O que vem a seguir?

Após analisar os requisitos de migração, você pode "[Prepare-se para migrar seus switches](#)".

Prepare-se para a migração de clusters sem switches para clusters com switches.

Siga estes passos para preparar seu cluster sem switch para a migração para um cluster com dois nós com switch.

Passos

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período 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

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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
e4a          n1_clus1    up/up      10.10.0.1/24      n1
true
e4e          n1_clus2    up/up      10.10.0.2/24      n1
true
e4a          n2_clus1    up/up      10.10.0.3/24      n2
true
e4e          n2_clus2    up/up      10.10.0.4/24      n2
true
4 entries were displayed.
```

3. Verifique se os RCFs e a imagem apropriados estão instalados nos novos switches 3132Q-V, conforme necessário para suas necessidades, e faça quaisquer personalizações essenciais do site, como usuários e senhas, endereços de rede e assim por diante.

Você deve preparar ambos os interruptores neste momento. Se precisar atualizar o RCF e o software de imagem, siga estes passos:

- a. Vá para ["Switches Ethernet da Cisco"](#) no site de suporte da NetApp .
 - b. Anote o modelo do seu switch e as versões de software necessárias na tabela dessa 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.
4. Selecione **CONTINUAR** na página **Descrição**, aceite o contrato de licença e siga as instruções na página **Download** para baixar o RCF.

O que vem a seguir?

Depois de se preparar para migrar seus switches, você pode ["configure suas portas"](#) .

Configure suas portas para migração de clusters sem switch para clusters com switch.

Siga estes passos para configurar suas portas para migração de clusters de dois nós sem switch para clusters de dois nós com switch.

Passos

1. Nos switches Nexus 3132Q-V C1 e C2, desative todas as portas voltadas para o nó C1 e C2, mas não desative as portas ISL.

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 sendo desativadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração compatível com o 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. Conecte as portas 1/31 e 1/32 em C1 às mesmas portas em C2 usando cabos compatíveis.
3. Verifique se as portas ISL estão operacionais em 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. Exibir 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. Exibir a conectividade da porta do cluster em cada nó:

```
network device-discovery show
```

Mostrar exemplo

O exemplo a seguir mostra uma configuração de cluster sem switch com dois nós.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered 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 a interface 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. Verificar 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. Desative as portas do 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde 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

Todas as versões do ONTAP

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

```
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. Desconecte o cabo de e4a no nó n1.

Você pode consultar a configuração em execução e conectar a primeira porta 40 GbE do switch C1 (porta 1/7 neste exemplo) à porta e4a do switch n1 usando os cabos compatíveis com o Nexus 3132Q-V.



Ao reconectar qualquer cabo a um novo switch de cluster Cisco , os cabos utilizados devem ser de fibra óptica ou cabos suportados pela Cisco.

2. Desconecte o cabo do e4a no nó n2.

Você pode consultar a configuração em execução e conectar o e4a à próxima porta 40 GbE disponível em C1, porta 1/8, usando cabos compatíveis.

3. Habilite todas as portas voltadas para o nó em C1.

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 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 do 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 as LIFs migradas sendo revertidas para suas portas de origem.

```
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 do cluster foram revertidas para suas portas originais:

```
network interface show
```

O Is Home A coluna deve exibir um valor de true para todos os portos listados no 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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a n1_clus1 up/up 10.10.0.1/24 n1
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. Exibir a conectividade 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 o 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. Desative as portas do cluster clus2 LIF em ambos os nós:

```
network port modify
```

O exemplo a seguir mostra as portas especificadas sendo desativadas 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 do 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
e4a          n1_clus1    up/up      10.10.0.1/24      n1
true
e4a          n1_clus2    up/up      10.10.0.2/24      n1
false
e4a          n2_clus1    up/up      10.10.0.3/24      n2
true
e4a          n2_clus2    up/up      10.10.0.4/24      n2
false
4 entries were displayed.
```

12. Desconecte o cabo do e4e no nó n1.

Você pode consultar a configuração em execução e conectar a primeira porta 40 GbE no switch C2 (porta 1/7 neste exemplo) à porta e4e em n1 usando cabeamento compatível no Nexus 3132Q-V.

13. Desconecte o cabo do e4e no nó n2.

Você pode consultar a configuração em execução e conectar o e4e à próxima porta 40 GbE disponível em C2, porta 1/8, usando cabos compatíveis.

14. Habilite todas as portas voltadas para o nó no C2.

Mostrar exemplo

O exemplo a seguir mostra as portas de 1 a 30 sendo habilitadas nos switches de cluster Nexus 3132Q-V C1 e C2 usando uma configuração compatível com o 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 ativadas:

```
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 as LIFs migradas sendo revertidas para suas portas de origem.

```
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 do cluster foram revertidas para suas portas originais:

```
network interface show
```

O `Is Home` A coluna deve exibir um valor de `true` para todos os portos listados no `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 do cluster estão configuradas corretamente. 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 vem a seguir?

Depois de configurar as portas do seu switch, você pode ["Conclua sua migração"](#) .

Conclua a migração de clusters de dois nós sem switch para clusters de dois nós com switch.

Siga estes passos para concluir a migração de clusters sem switches para clusters com switches de dois nós.

Passos

1. Exibir os números das portas do switch de cluster às quais cada porta do cluster está conectada em cada nó:

network device-discovery show

Mostrar exemplo

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered 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 os switches de cluster descobertos e monitorados:

system cluster-switch show

Mostrar exemplo

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
C1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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 de configuração sem switch para dois nós em qualquer um dos nós:

```
network options switchless-cluster
```

```
network options switchless-cluster modify -enabled false
```

4. Verifique se o switchless-cluster Essa opção foi desativada.

```
network options switchless-cluster show
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde 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

Todas as versões do ONTAP

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

```
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. [[passo 6]]Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

O que vem a seguir?

Após concluir a migração do seu switch, você poderá [configurar monitoramento de integridade do switch](#) .

Substitua os interruptores

Requisitos para substituição de switches de cluster Cisco Nexus 3132Q-V

Ao substituir switches de cluster, certifique-se de compreender os requisitos de configuração, as conexões de porta e os requisitos de cabeamento.

Requisitos do Cisco Nexus 3132Q-V

- O switch de cluster Cisco Nexus 3132Q-V é compatível.
- O número de portas 10 GbE e 40 GbE está definido nos arquivos de configuração de referência (RCFs) disponíveis em [Download do arquivo de configuração de referência do switch de rede de cluster Cisco](#) .

- Os switches do cluster utilizam as portas Inter-Switch Link (ISL) e1/31-32.
- O ["Hardware Universe"](#) Contém informações sobre a cablagem compatível com os switches Nexus 3132Q-V:
 - Os nós com conexões de cluster de 10 GbE requerem módulos ópticos QSFP com cabos de fibra óptica breakout ou cabos breakout de cobre QSFP para SFP+.
 - Os nós com conexões de cluster de 40 GbE requerem módulos ópticos QSFP/QSFP28 compatíveis com cabos de fibra óptica ou cabos de cobre QSFP/QSFP28 de conexão direta.
 - Os switches do cluster utilizam a cablagem ISL apropriada: 2 cabos de fibra óptica QSFP28 ou cabos de cobre de ligação direta.
- No Nexus 3132Q-V, você pode operar as portas QSFP nos 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 seguindo uma convenção de nomenclatura de 2 elementos. Por exemplo, a segunda porta Ethernet de 40 Gb é numerada como 1/2. O processo de alterar a configuração de Ethernet de 40 Gb para Ethernet de 10 Gb é chamado de *breakout* e o processo de alterar a configuração de Ethernet de 10 Gb para Ethernet de 40 Gb é chamado de *breakin*. Ao dividir uma porta Ethernet de 40 Gb em portas Ethernet de 10 Gb, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 elementos. Por exemplo, as portas de conexão da segunda porta Ethernet de 40 Gb são numeradas como 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- No lado esquerdo do Nexus 3132Q-V encontra-se 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 no Nexus 3132Q-V usando o seguinte: `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 deve ter configurado algumas das portas do Nexus 3132Q-V para funcionar em 10 GbE ou 40 GbE.

Você pode configurar as seis primeiras portas para o modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as seis primeiras portas QSFP+ da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você deve ter realizado o planejamento, a migração e lido a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.

["Switches Ethernet da Cisco"](#) Contém informações sobre as versões do ONTAP e do NX-OS suportadas neste procedimento.

Requisitos do Cisco Nexus 5596

- Os seguintes switches de cluster são suportados:
 - Nexus 5596
 - Nexus 3132Q-V
- O número de portas 10 GbE e 40 GbE está definido nos arquivos de configuração de referência (RCFs)

disponíveis em ["Download do arquivo de configuração de referência do switch de rede de cluster Cisco"](#) .

- Os switches do cluster utilizam as seguintes portas para conexões com os nós:
 - Portas e1/1-40 (10 GbE): Nexus 5596
 - Portas e1/1-30 (40 GbE): Nexus 3132Q-V
- Os switches do cluster utilizam as seguintes portas de Inter-Switch Link (ISL):
 - Portas e1/41-48 (10 GbE): Nexus 5596
 - Portas e1/31-32 (40 GbE): Nexus 3132Q-V
- O ["Hardware Universe"](#) Contém informações sobre a cablagem compatível com os switches Nexus 3132Q-V:
 - Os nós com conexões de cluster de 10 GbE requerem cabos breakout de fibra óptica QSFP para SFP+ ou cabos breakout de cobre QSFP para SFP+.
 - Os nós com conexões de cluster de 40 GbE requerem módulos ópticos QSFP/QSFP28 compatíveis com cabos de fibra óptica ou cabos de cobre QSFP/QSFP28 de conexão direta.
- Os switches do cluster utilizam a cablagem ISL apropriada:
 - Início: Nexus 5596 para Nexus 5596 (SFP+ para SFP+)
 - 8 cabos de conexão direta SFP+ em fibra óptica ou cobre
 - Interino: Nexus 5596 para Nexus 3132Q-V (adaptador QSFP para 4xSFP+)
 - 1 cabo breakout de fibra óptica ou de cobre QSFP para SFP+
 - Versão final: Nexus 3132Q-V para Nexus 3132Q-V (QSFP28 para QSFP28)
 - 2 cabos de fibra óptica ou cobre QSFP28 com conexão direta
- Nos switches Nexus 3132Q-V, você pode operar as portas QSFP/QSFP28 nos modos 40 Gigabit Ethernet ou 4 x10 Gigabit Ethernet.

Por padrão, existem 32 portas no modo Ethernet de 40 Gigabit. Essas 40 portas Gigabit Ethernet são numeradas seguindo uma convenção de nomenclatura de 2 elementos. Por exemplo, a segunda porta Ethernet de 40 Gigabits é numerada como 1/2. O processo de alterar a configuração de Ethernet de 40 Gigabit para Ethernet de 10 Gigabit é chamado de *breakout* e o processo de alterar a configuração de Ethernet de 10 Gigabit para Ethernet de 40 Gigabit é chamado de *breakin*. Ao dividir uma porta Ethernet de 40 Gigabits em portas Ethernet de 10 Gigabits, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 elementos. Por exemplo, as portas de conexão da segunda porta Ethernet de 40 Gigabit são numeradas como 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- No lado esquerdo dos switches Nexus 3132Q-V, há um conjunto de 4 portas SFP+ multiplexadas para essa porta QSFP28.

Por padrão, o RCF é configurado para usar a porta QSFP28.



Você pode ativar 4 portas SFP+ em vez de uma porta QSFP nos switches Nexus 3132Q-V usando o seguinte: `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 4 portas SFP+ usando o `hardware profile front portmode qsfp` comando.

- Você configurou algumas portas nos switches Nexus 3132Q-V para operar em 10 GbE ou 40 GbE.



Você pode configurar as seis primeiras portas para o modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as seis primeiras portas QSFP+ da configuração de breakout usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você já realizou 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 do ONTAP e do NX-OS suportadas neste procedimento são as seguintes: "[Switches Ethernet da Cisco](#)".

Requisitos do NetApp CN1610

- Os seguintes switches de cluster são suportados:
 - NetApp CN1610
 - Cisco Nexus 3132Q-V
- Os switches de cluster suportam as seguintes conexões de nó:
 - NetApp CN1610: portas 0/1 a 0/12 (10 GbE)
 - Cisco Nexus 3132Q-V: portas e1/1-30 (40 GbE)
- Os switches do cluster utilizam as seguintes portas de enlace entre switches (ISL):
 - NetApp CN1610: portas 0/13 a 0/16 (10 GbE)
 - Cisco Nexus 3132Q-V: portas e1/31-32 (40 GbE)
- O "[Hardware Universe](#)" contém informações sobre a cablagem compatível com os switches Nexus 3132Q-V:
 - Os nós com conexões de cluster de 10 GbE requerem cabos breakout de fibra óptica QSFP para SFP+ ou cabos breakout de cobre QSFP para SFP+.
 - Os nós com conexões de cluster de 40 GbE requerem módulos ópticos QSFP/QSFP28 compatíveis com cabos de fibra óptica ou cabos de cobre QSFP/QSFP28 de conexão direta.
- A cablagem ISL adequada é a seguinte:
 - Início: Para CN1610 a CN1610 (SFP+ a SFP+), quatro cabos de fibra óptica ou cobre SFP+ de conexão direta.
 - Provisório: Para CN1610 para Nexus 3132Q-V (conversor QSFP para quatro SFP+), um cabo de fibra óptica ou cobre com conversor QSFP para SFP+.
 - Final: Para conexão direta entre Nexus 3132Q-V e Nexus 3132Q-V (QSFP28 para QSFP28), utilize dois cabos de fibra óptica ou cobre QSFP28.
- Os cabos twinax da NetApp não são compatíveis com os switches Cisco Nexus 3132Q-V.

Se a sua configuração atual do CN1610 utiliza cabos twinax da NetApp para conexões entre nós do cluster e switches ou conexões ISL, e você deseja continuar usando twinax em seu ambiente, será necessário adquirir cabos twinax da Cisco. Alternativamente, você pode usar cabos de fibra óptica tanto para as conexões ISL quanto para as conexões entre os nós do cluster e os switches.

- Nos switches Nexus 3132Q-V, você pode operar as portas QSFP/QSFP28 nos 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 seguindo uma convenção de nomenclatura de 2 elementos. Por exemplo, a segunda porta

Ethernet de 40 Gb é numerada como 1/2. O processo de alterar a configuração de Ethernet de 40 Gb para Ethernet de 10 Gb é chamado de *breakout* e o processo de alterar a configuração de Ethernet de 10 Gb para Ethernet de 40 Gb é chamado de *breakin*. Ao dividir uma porta Ethernet de 40 Gb em portas Ethernet de 10 Gb, as portas resultantes são numeradas usando uma convenção de nomenclatura de 3 elementos. Por exemplo, as portas de conexão da segunda porta Ethernet de 40 Gb são numeradas como 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- No lado esquerdo dos switches Nexus 3132Q-V, encontra-se 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.

É possível ativar quatro portas SFP+ em vez de uma porta QSFP nos switches Nexus 3132Q-V usando o seguinte: `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.



Ao utilizar as quatro primeiras portas SFP+, a primeira porta QSFP de 40GbE será desativada.

- Você deve ter configurado algumas das portas nos switches Nexus 3132Q-V para funcionar em 10 GbE ou 40 GbE.

Você pode configurar as seis primeiras portas para o modo 4x10 GbE usando o `interface breakout module 1 port 1-6 map 10g-4x` comando. Da mesma forma, você pode reagrupar as seis primeiras portas QSFP+ da configuração *breakout* usando o `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Você deve ter realizado o planejamento, a migração e lido a documentação necessária sobre a conectividade de 10 GbE e 40 GbE dos nós para os switches de cluster Nexus 3132Q-V.
- As versões do ONTAP e do NX-OS suportadas neste procedimento estão listadas em "[Switches Ethernet da Cisco](#)".
- As versões do ONTAP e do FASTPATH compatíveis com este procedimento estão listadas em "[Switches NetApp CN1601 e CN1610](#)".

Substitua os switches de cluster Cisco Nexus 3132Q-V

Siga este procedimento para substituir um switch Cisco Nexus 3132Q-V defeituoso em uma rede cluster. O procedimento de substituição é um procedimento não disruptivo (NDO).

Requisitos de revisão

Requisitos do switch

Analise o "[Requisitos para substituição de switches de cluster Cisco Nexus 3132Q-V](#)".

Antes de começar

- A configuração de cluster e rede existente apresenta:
 - A infraestrutura do cluster Nexus 3132Q-V é redundante e totalmente funcional em ambos os switches.

"[Switch Ethernet Cisco](#)" Possui as versões mais recentes do RCF e do NX-OS para seus switches.

- Todas as portas do cluster estão no `up` estado.
- A conectividade de gerenciamento existe em ambos os switches.
- Todas as interfaces lógicas do cluster (LIFs) estão no `up` estado e foram migrados.
- Para o switch de substituição Nexus 3132Q-V, certifique-se de que:
 - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
 - O acesso ao console para o interruptor de substituição já está instalado.
 - A imagem desejada do sistema operacional RCF e NX-OS é carregada no switch.
 - A personalização inicial do interruptor está concluída.
- ["Hardware Universe"](#)

Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

Substitua o interruptor

Este procedimento substitui o segundo interruptor de cluster Nexus 3132Q-V CL2 pelo novo interruptor 3132Q-V C2.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- `n1_clus1` é a primeira interface lógica de cluster (LIF) conectada ao switch de cluster C1 para o nó `n1`.
- `n1_clus2` é a primeira LIF de cluster conectada ao switch de cluster CL2 ou C2, para o nó `n1`.
- `n1_clus3` é a segunda LIF conectada ao switch de cluster C2, para o nó `n1`.
- `n1_clus4` é a segunda LIF conectada ao switch de cluster CL1, para o nó `n1`.
- O número de portas 10 GbE e 40 GbE está definido nos arquivos de configuração de referência (RCFs) disponíveis em ["Download do arquivo de configuração de referência do switch 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 o ["Hardware Universe"](#) para obter as portas de cluster reais em 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 interruptor de cluster CL2 será substituído por C2.
 - Em cada nó, as LIFs do cluster conectadas ao CL2 são migradas para as portas do cluster conectadas ao CL1.
 - Desconecte os cabos de todas as portas do CL2 e reconecte-os às mesmas portas no switch de substituição C2.
 - Em cada nó, os LIFs (Life-Input Factors) de cluster migrados são revertidos.

Etapa 1: Prepare-se para a substituição

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Exibir informações sobre os dispositivos na 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			Link	MTU	Admin/Oper	
Port	IPspace	Broadcast	Domain				
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			Link	MTU	Admin/Oper	
Port	IPspace	Broadcast	Domain				
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

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)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0b	n1_clus2	up/up	10.10.0.2/24	n1
e0c	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0b	n2_clus2	up/up	10.10.0.6/24	n2
e0c	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e0a	n3_clus1	up/up	10.10.0.9/24	n3
e0e	n3_clus2	up/up	10.10.0.10/24	n3
e0a	n4_clus1	up/up	10.10.0.11/24	n4
e0e	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

c. Exibir as informações sobre os switches de cluster descobertos:

```
system cluster-switch show
```

Mostrar exemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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 para suas necessidades, e faça quaisquer personalizações essenciais no local.

Você deve preparar o interruptor de substituição neste momento. Se precisar atualizar o RCF e a imagem, siga estes passos:

- a. No site de suporte da NetApp, consulte ["Switches Ethernet da Cisco"](#).
 - b. Anote o modelo do seu switch e as versões de software necessárias na tabela dessa página.
 - c. Faça o download da 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. Baixe a versão apropriada do software de imagem.
5. Migre as LIFs associadas às portas do cluster conectadas ao switch C2:

```
network interface migrate
```


Mostrar exemplo

Este exemplo mostra que a migração LIF foi realizada 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. Verificar a integridade do cluster:

```
network interface show
```

Mostrar exemplo

```
cluster::*> network interface show -role cluster
(network interface show)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0a	n1_clus2	up/up	10.10.0.2/24	n1
e0d	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0a	n2_clus2	up/up	10.10.0.6/24	n2
e0d	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e4a	n3_clus1	up/up	10.10.0.9/24	n3
e4a	n3_clus2	up/up	10.10.0.10/24	n3
e4a	n4_clus1	up/up	10.10.0.11/24	n4
e4a	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

7. Desative as portas de interconexão do cluster que estão fisicamente conectadas ao switch CL2:

```
network port modify
```

Mostrar exemplo

Este exemplo mostra as portas especificadas sendo desativadas 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o comando `show` para exibir os detalhes.

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

Node	Date	Source LIF	Destination LIF	Packet 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				
...				
...				

Todas as versões do ONTAP

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

```
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. [[passo 9]]Desligue as portas 1/31 e 1/32 em CL1 e o switch Nexus 3132Q-V ativo:

```
shutdown
```

Mostrar exemplo

Este exemplo mostra as portas ISL 1/31 e 1/32 sendo desativadas no switch 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 conectados ao switch Nexus 3132Q-V CL2 e reconecte-os ao switch de substituição C2 em todos os nós.
2. Remova os cabos ISL das portas e1/31 e e1/32 do CL2 e reconecte-os às mesmas portas no switch de substituição C2.
3. Ative as portas ISL 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 ativos no CL1:

```
show port-channel
```

As portas Eth1/31 e Eth1/32 devem indicar (P) , o que significa que as portas ISL estão ativas no canal de portas.

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 ativos no C2:

```
show port-channel summary
```

As portas Eth1/31 e Eth1/32 devem indicar (P) , o que significa que ambas as portas ISL estão ativas 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, ative todas as portas de interconexão do cluster conectadas 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 do cluster foram revertidas para seus valores originais:

```
network interface show
```


Mostrar exemplo

Este exemplo mostra que todas as LIFs foram revertidas com sucesso porque as portas listadas em Current Port a coluna tem o status de true no Is Home coluna. Se o Is Home o valor da coluna é 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 conectadas:

```
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o comando `show` para exibir os detalhes.

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

Node	Date	Source LIF	Destination LIF	Packet 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				
...				
...				

Todas as versões do ONTAP

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

```
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)
```

Etapas 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 Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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 NX3132V	cluster-network	10.10.1.103
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. Remova o switch Nexus 3132Q-V substituído, caso ele ainda não tenha sido removido automaticamente:

```
system cluster-switch delete
```

```
cluster::*> system cluster-switch delete -device CL2
```

3. Verifique se os switches de cluster apropriados estão sendo 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 desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

O que vem a seguir?

Depois de substituir o interruptor, você pode ["configurar monitoramento de integridade do switch"](#) .

Substituir switches de cluster Cisco Nexus 3132Q-V por conexões sem switch

No ONTAP 9.3 e versões posteriores, é possível migrar de um cluster com uma rede de cluster comutada para um cluster onde dois nós estão conectados diretamente.

A NetApp recomenda que você atualize a versão do seu ONTAP antes de prosseguir com a operação de cluster comutado para cluster sem switch para switches Cisco Nexus 3132Q-V.



Veja o seguinte para mais detalhes:

- ["SU540: Erros na placa de rede Chelsio T6 causam desligamento do sistema ao atualizar switches de rede de 40G para 100G"](#)
- ["Pânico no nó após migração de cluster com switch para cluster sem switch"](#)

É possível migrar de um cluster com uma rede de cluster comutada para uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

Requisitos de revisão

Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

Antes de começar

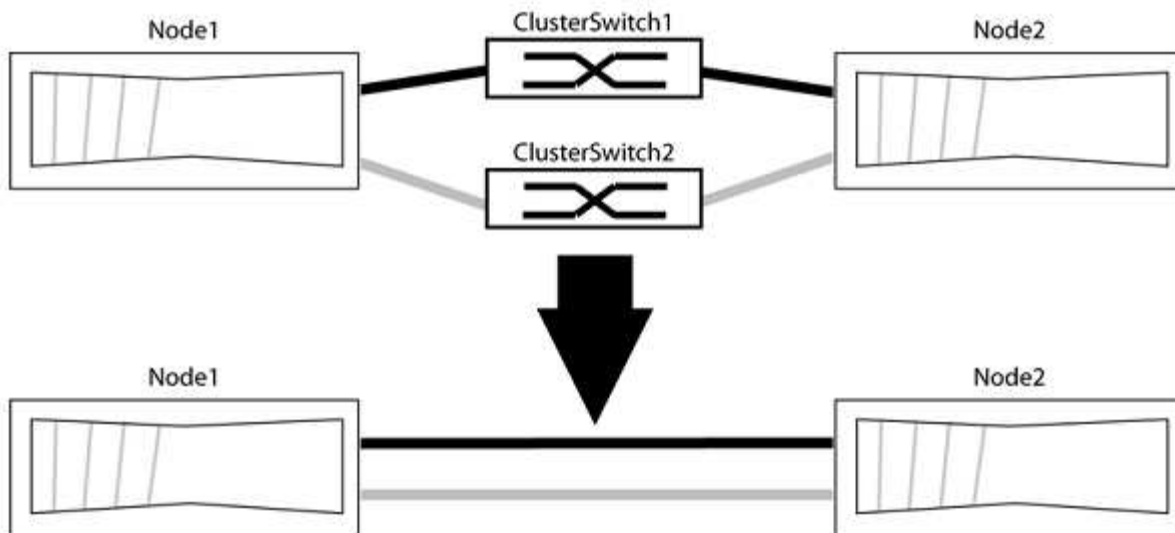
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

Migre 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 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 elas variam de acordo com o sistema.

Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message  
MAINT=<number_of_hours>h
```

onde *h* é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

Mostrar exemplo

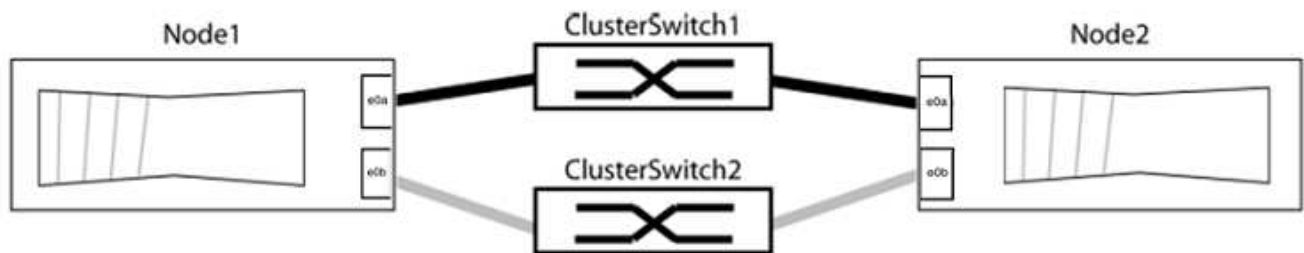
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de *up* para a coluna "Link" e um valor de *healthy* para a coluna "Estado de Saúde".

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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está `true` para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

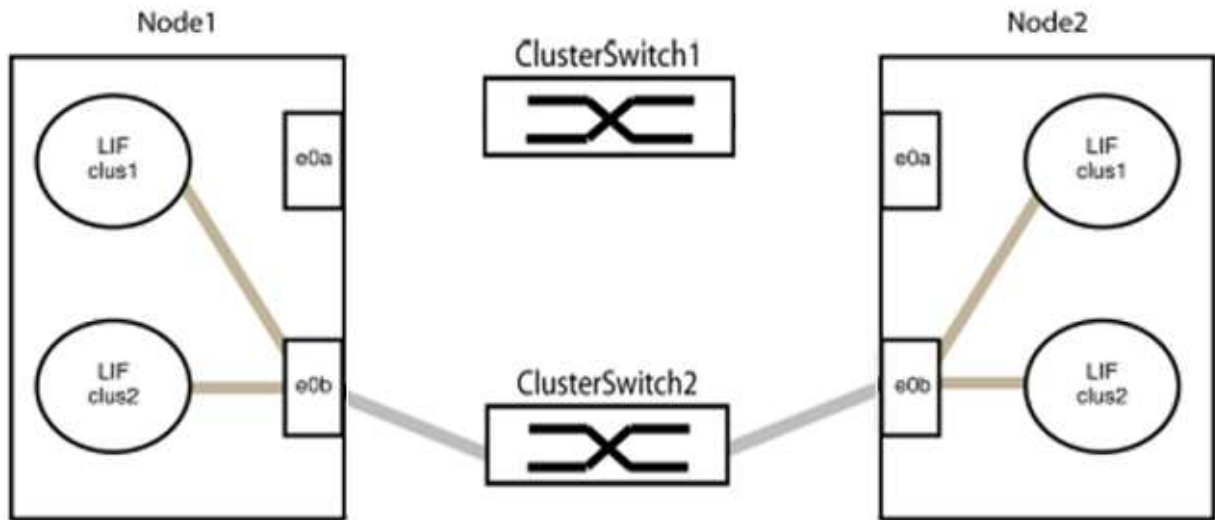
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

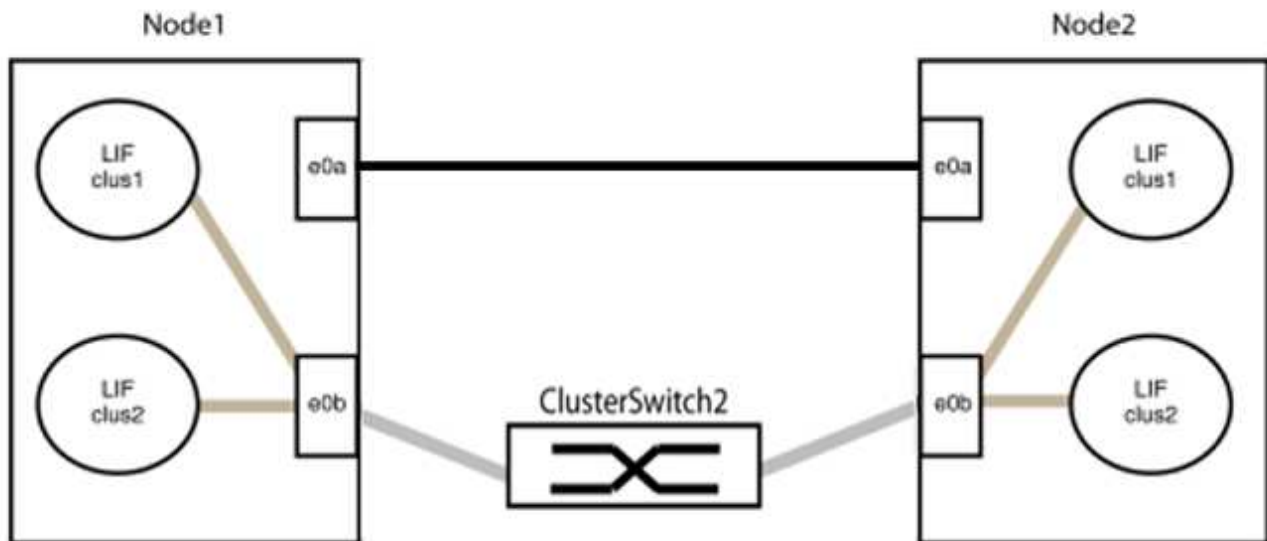
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

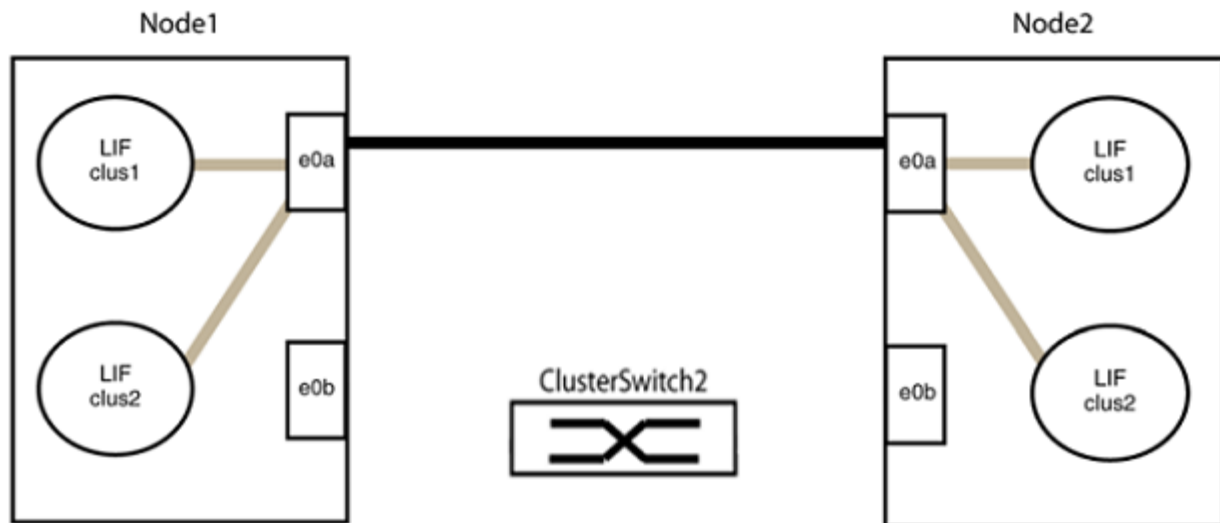
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

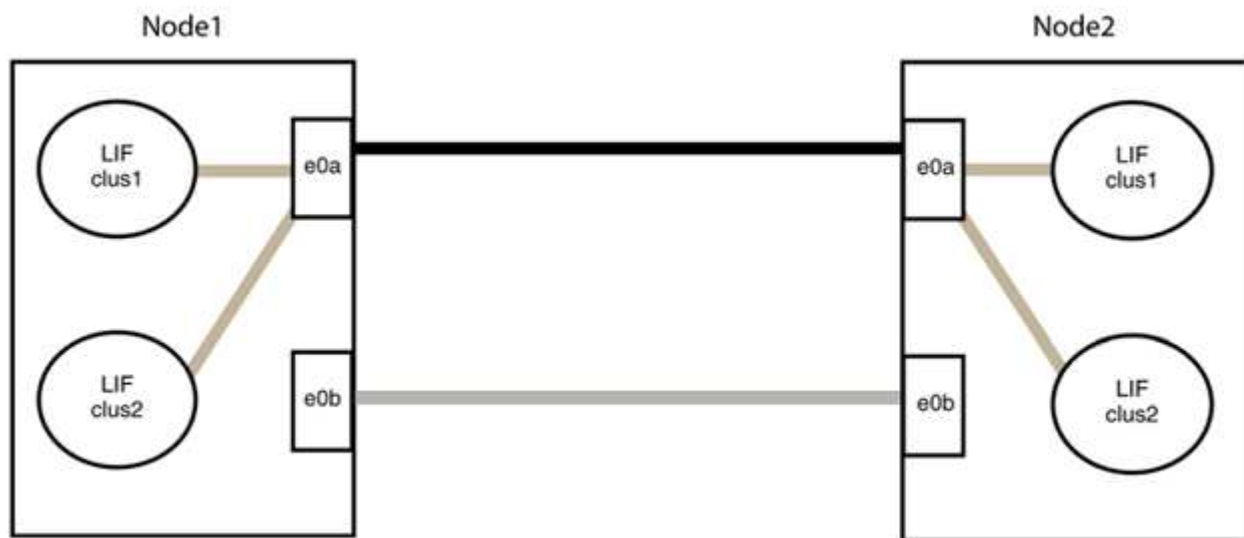
- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna "Is Home" estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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
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		

Todas as versões do ONTAP

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

```
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. [[passo 6]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

Cisco Nexus 92300YC

Começar

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 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.

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 a instalação e manutenção do switch Cisco Nexus 92300YC, certifique-se de revisar todos os requisitos de configuração e de rede.

Se você deseja criar clusters ONTAP com mais de dois nós, precisará de dois switches de rede de cluster compatíveis. Você pode usar interruptores de gerenciamento adicionais, que são opcionais.

Requisitos de configuração

Para configurar seu cluster, você precisa da quantidade e do tipo adequados de cabos e conectores de cabos para seus switches. Dependendo do tipo de switch que você estiver configurando inicialmente, será necessário conectar-se à porta de console do switch com o cabo de console incluído; você também precisará fornecer informações específicas da rede.

Requisitos de rede

Você precisa das seguintes informações de rede para todas as configurações de switch:

- Sub-rede IP para tráfego de rede de gerenciamento
- Nomes de host e endereços IP para cada um dos controladores do sistema de armazenamento e todos os switches aplicáveis
- A maioria dos controladores de sistema de armazenamento são gerenciados por meio da interface e0M,

conectando-se à porta de serviço Ethernet (ícone de chave inglesa). Nos sistemas AFF A800 e AFF A700 , a interface eOM utiliza uma porta Ethernet dedicada.

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

O que vem a seguir

Após analisar os requisitos de configuração, você poderá confirmar sua solicitação. ["componentes e números de peças"](#).

Componentes e números de peça para switches Cisco Nexus 92300YC

Para a instalação e manutenção do switch Cisco Nexus 92300YC, certifique-se de revisar todos os componentes e números de peça do switch. Consulte o ["Hardware Universe"](#) para obter detalhes. Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação do switch.

A tabela a seguir lista o número da peça e a descrição do switch 92300YC, dos ventiladores e das fontes de alimentação:

Número da peça	Descrição
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = Exaustão do Lado da Porta)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = Entrada do Lado da Porta)
X-NXA-FAN-35CFM-B	Ventilador, entrada de ar lateral da porta Cisco N9K
X-NXA-FAN-35CFM-F	Ventilador, fluxo de ar de exaustão lateral da porta Cisco N9K
X-NXA-PAC-650W-B	Fonte de alimentação Cisco 650W - entrada lateral
X-NXA-PAC-650W-F	Fonte de alimentação Cisco 650W - exaustão lateral.

Detalhes do fluxo de ar do switch Cisco Nexus 92300YC:

- Fluxo de ar de exaustão pelo lado esquerdo (ar padrão) — O ar frio entra no chassi através dos módulos de ventoinha e fonte de alimentação no corredor frio e é expelido pela extremidade esquerda do chassi no corredor quente. Fluxo de ar de exaustão do lado de bombordo com coloração azul.
- Fluxo de ar de entrada pelo lado esquerdo (ar reverso) — O ar frio entra no chassi pela extremidade esquerda no corredor frio e é expelido através do ventilador e dos módulos de alimentação no corredor quente. Fluxo de ar de admissão pelo lado esquerdo com coloração bordô.

O que vem a seguir

Após confirmar os componentes e os números de peça, você pode revisar o ["documentação necessária"](#).

Requisitos de documentação para switches Cisco Nexus 92300YC

Para a instalação do switch Cisco Nexus 92300YC, certifique-se de revisar toda a documentação recomendada.

Documentação do Switch

Para configurar os switches Cisco Nexus 92300YC, você precisa da seguinte documentação de ["Suporte para switches Cisco Nexus série 9000"](#).

Título do documento	Descrição
<i>Guia de Instalação de Hardware da Série Nexus 9000</i>	Fornece informações detalhadas sobre os requisitos do local, detalhes do hardware do switch e opções de instalação.
<i>Guias de Configuração de Software para Switches Cisco Nexus Série 9000</i> (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece as informações iniciais de configuração do switch necessárias antes de configurá-lo para operação com ONTAP .
Guia de atualização e downgrade do software NX-OS da série Cisco Nexus 9000 (escolha o guia correspondente à versão do NX-OS instalada em seus switches)	Fornece informações sobre como fazer o downgrade do software do switch para uma versão compatível com ONTAP , se necessário.
<i>Índice principal de referência de comandos do Cisco Nexus 9000 Series NX-OS</i>	Fornece links para as diversas referências de comandos disponibilizadas pela Cisco.
<i>Referência de MIBs do Cisco Nexus 9000</i>	Descreve os arquivos da Base de Informações de Gerenciamento (MIB) para os switches Nexus 9000.
<i>Referência de mensagens do sistema NX-OS da série Nexus 9000</i>	Descreve as mensagens do sistema para switches da série Cisco Nexus 9000, incluindo as informativas e outras que podem ajudar a diagnosticar problemas com links, hardware interno ou software do sistema.
<i>Notas de versão do NX-OS para a série Cisco Nexus 9000</i> (selecione as notas referentes à versão do NX-OS instalada em seus switches)	Descreve as funcionalidades, os erros e as limitações da série Cisco Nexus 9000.
Informações sobre conformidade regulamentar e segurança para a série Cisco Nexus 9000	Fornece informações sobre conformidade com agências internacionais, segurança e regulamentações para os switches da série Nexus 9000.

Documentação dos sistemas ONTAP

Para configurar um sistema ONTAP, você precisa dos seguintes documentos para a sua versão do sistema operacional.

Nome	Descrição
Instruções de instalação e configuração específicas do controlador	Descreve como instalar o hardware da NetApp .
"ONTAP 9"	Fornecer informações detalhadas sobre todos os aspectos das versões do ONTAP .
"Hardware Universe"	Fornecer informações sobre configuração e compatibilidade de hardware da NetApp .

Kit de trilhos e documentação do gabinete

Para instalar um switch Cisco Nexus 92300YC em um NetApp cabinet, consulte a seguinte documentação de hardware.

Nome	Descrição
"Gabinete de sistema 42U, guia profundo"	Descreve as FRUs (Unidades Substituíveis em Campo) associadas ao gabinete do sistema 42U e fornece instruções de manutenção e substituição de FRUs.
"Instale um switch Cisco Nexus 92300YC em um gabinete NetApp ."	Este manual descreve como instalar um switch Cisco Nexus 92300YC em um gabinete NetApp de quatro postes.

Requisitos do 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:

- É necessário ter um servidor de e-mail instalado.
- O switch deve ter conectividade IP com o servidor de e-mail.
- É necessário configurar o nome do contato (contato do servidor SNMP), o número de telefone e o endereço. Isso é necessário para determinar a origem das mensagens recebidas.

- Um ID CCO deve estar associado a um contrato de serviço Cisco SMARTnet apropriado para sua empresa.
- O serviço Cisco SMARTnet deve estar instalado para que o dispositivo seja registrado.

O ["Site de suporte da Cisco"](#) Contém informações sobre os comandos para configurar o Smart Call Home.

Instalar 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 cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

2

"Instale o interruptor"

Instale o switch 92300YC.

3

"Instale o switch em um gabinete NetApp."

Instale o switch 92300YC e o painel de passagem em um gabinete NetApp , conforme necessário.

4

"Revisar a cablagem e a configuração."

Revise o suporte para portas Ethernet NVIDIA .

Folha de trabalho completa de cabeamento do Cisco Nexus 92300YC

Se você deseja documentar as plataformas suportadas, baixe o PDF desta página e preencha a planilha de cabeamento.

A planilha de cabeamento de exemplo fornece exemplos de atribuições de portas recomendadas dos switches aos controladores. A planilha em branco fornece um modelo que você pode usar para configurar seu cluster.

Exemplo de folha de exercícios de cabeamento

A definição da porta de exemplo em cada par de switches é a seguinte:

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós e portas	Porta de comutação	Utilização de nós e portas
1	Nó 10/25 GbE	1	Nó 10/25 GbE

Chave seletora de cluster A		Chave seletora de cluster B	
2	Nó 10/25 GbE	2	Nó 10/25 GbE
3	Nó 10/25 GbE	3	Nó 10/25 GbE
4	Nó 10/25 GbE	4	Nó 10/25 GbE
5	Nó 10/25 GbE	5	Nó 10/25 GbE
6	Nó 10/25 GbE	6	Nó 10/25 GbE
7	Nó 10/25 GbE	7	Nó 10/25 GbE
8	Nó 10/25 GbE	8	Nó 10/25 GbE
9	Nó 10/25 GbE	9	Nó 10/25 GbE
10	Nó 10/25 GbE	10	Nó 10/25 GbE
11	Nó 10/25 GbE	11	Nó 10/25 GbE
12	Nó 10/25 GbE	12	Nó 10/25 GbE
13	Nó 10/25 GbE	13	Nó 10/25 GbE
14	Nó 10/25 GbE	14	Nó 10/25 GbE
15	Nó 10/25 GbE	15	Nó 10/25 GbE
16	Nó 10/25 GbE	16	Nó 10/25 GbE
17	Nó 10/25 GbE	17	Nó 10/25 GbE
18	Nó 10/25 GbE	18	Nó 10/25 GbE
19	Nó 10/25 GbE	19	Nó 10/25 GbE
20	Nó 10/25 GbE	20	Nó 10/25 GbE
21	Nó 10/25 GbE	21	Nó 10/25 GbE
22	Nó 10/25 GbE	22	Nó 10/25 GbE
23	Nó 10/25 GbE	23	Nó 10/25 GbE

Chave seletora de cluster A		Chave seletora de cluster B	
24	Nó 10/25 GbE	24	Nó 10/25 GbE
25	Nó 10/25 GbE	25	Nó 10/25 GbE
26	Nó 10/25 GbE	26	Nó 10/25 GbE
27	Nó 10/25 GbE	27	Nó 10/25 GbE
28	Nó 10/25 GbE	28	Nó 10/25 GbE
29	Nó 10/25 GbE	29	Nó 10/25 GbE
30	Nó 10/25 GbE	30	Nó 10/25 GbE
31	Nó 10/25 GbE	31	Nó 10/25 GbE
32	Nó 10/25 GbE	32	Nó 10/25 GbE
33	Nó 10/25 GbE	33	Nó 10/25 GbE
34	Nó 10/25 GbE	34	Nó 10/25 GbE
35	Nó 10/25 GbE	35	Nó 10/25 GbE
36	Nó 10/25 GbE	36	Nó 10/25 GbE
37	Nó 10/25 GbE	37	Nó 10/25 GbE
38	Nó 10/25 GbE	38	Nó 10/25 GbE
39	Nó 10/25 GbE	39	Nó 10/25 GbE
40	Nó 10/25 GbE	40	Nó 10/25 GbE
41	Nó 10/25 GbE	41	Nó 10/25 GbE
42	Nó 10/25 GbE	42	Nó 10/25 GbE
43	Nó 10/25 GbE	43	Nó 10/25 GbE
44	Nó 10/25 GbE	44	Nó 10/25 GbE
45	Nó 10/25 GbE	45	Nó 10/25 GbE

Chave seletora de cluster A		Chave seletora de cluster B	
46	Nó 10/25 GbE	46	Nó 10/25 GbE
47	Nó 10/25 GbE	47	Nó 10/25 GbE
48	Nó 10/25 GbE	48	Nó 10/25 GbE
49	Nó 40/100 GbE	49	Nó 40/100 GbE
50	Nó 40/100 GbE	50	Nó 40/100 GbE
51	Nó 40/100 GbE	51	Nó 40/100 GbE
52	Nó 40/100 GbE	52	Nó 40/100 GbE
53	Nó 40/100 GbE	53	Nó 40/100 GbE
54	Nó 40/100 GbE	54	Nó 40/100 GbE
55	Nó 40/100 GbE	55	Nó 40/100 GbE
56	Nó 40/100 GbE	56	Nó 40/100 GbE
57	Nó 40/100 GbE	57	Nó 40/100 GbE
58	Nó 40/100 GbE	58	Nó 40/100 GbE
59	Nó 40/100 GbE	59	Nó 40/100 GbE
60	Nó 40/100 GbE	60	Nó 40/100 GbE
61	Nó 40/100 GbE	61	Nó 40/100 GbE
62	Nó 40/100 GbE	62	Nó 40/100 GbE
63	Nó 40/100 GbE	63	Nó 40/100 GbE
64	Nó 40/100 GbE	64	Nó 40/100 GbE
65	ISL de 100 GbE para a porta 65 do switch B	65	ISL de 100 GbE para switch A porta 65
66	ISL de 100 GbE para a porta 66 do switch B	66	ISL de 100 GbE para switch A porta 65

Folha de exercícios de cabeamento em branco

Você pode usar a planilha de cabeamento em branco para documentar as plataformas suportadas como nós em um cluster. A seção *Conexões de Cluster Suportadas* do "[Hardware Universe](#)" define as portas de cluster usadas pela plataforma.

Chave seletora de cluster A		Chave seletora de cluster B	
Porta de comutação	Utilização de nós/portas	Porta de comutação	Utilização de nós/portas
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	

Chave seletora de cluster A		Chave seletora de cluster B	
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	
37		37	
38		38	
39		39	
40		40	
41		41	

Chave seletora de cluster A		Chave seletora de cluster B	
42		42	
43		43	
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	

Chave seletora de cluster A		Chave seletora de cluster B	
64		64	
65	ISL para switch B porta 65	65	ISL para comutar a porta A 65
66	ISL para comutador B porta 66	66	ISL para comutar a porta A 66

O que vem a seguir

Depois de concluir suas planilhas de cabeamento, você pode ["instalar o interruptor"](#).

Instalar o switch de cluster 92300YC

Siga este procedimento para instalar e configurar o switch Cisco Nexus 92300YC.

Antes de começar

Certifique-se de ter o seguinte:

- Acesso a um servidor HTTP, FTP ou TFTP no local de instalação para baixar as versões aplicáveis do NX-OS e do Arquivo de Configuração de Referência (RCF).
- Versão aplicável do NX-OS, baixada de ["Download do software Cisco"](#) página.
- Licenças aplicáveis, informações de rede e configuração, e cabos.
- Concluído ["Folhas de exercícios de cabeamento"](#).
- Os RCFs aplicáveis para rede de cluster e rede de gerenciamento da NetApp foram baixados do site de suporte da NetApp em ["meusuporte.netapp.com"](#). Todos os switches de rede de cluster e de gerenciamento da Cisco são entregues com a configuração padrão de fábrica da Cisco. Esses switches também têm a versão atual do software NX-OS, mas não têm os RCFs carregados.
- ["Documentação necessária sobre switches e ONTAP"](#).

Passos

1. Instale os switches e controladores da rede de cluster e da rede de gerenciamento no rack.

Se você estiver instalando o...	Então...
Cisco Nexus 92300YC em um gabinete de sistema NetApp	Consulte o guia <i>Instalando um switch de cluster Cisco Nexus 92300YC e um painel de passagem em um gabinete NetApp</i> para obter instruções sobre como instalar o switch em um gabinete NetApp.
Equipamentos em um rack de telecomunicações	Consulte os procedimentos fornecidos nos guias de instalação do hardware do switch e nas instruções de instalação e configuração da NetApp.

2. Conecte os switches da rede do cluster e da rede de gerenciamento aos controladores usando as planilhas de cabeamento preenchidas.
3. Ligue os switches e controladores da rede do cluster e da rede de gerenciamento.

O que vem a seguir?

Opcionalmente, você pode ["instalar um switch Cisco Nexus 3223C em um gabinete NetApp"](#). Caso contrário, acesse ["Revisar a cablagem 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 em ["Guia de Instalação de Hardware da Série Cisco Nexus 9000"](#) .
- Para cada interruptor, são necessários oito parafusos 10-32 ou 12-24 e porcas de fixação para montar os suportes e trilhos deslizantes nos postes dianteiro e traseiro do gabinete.
- Kit de trilhos padrão da Cisco para instalar o switch em um gabinete NetApp .



Os cabos de ligação não estão incluídos no kit de passagem e devem ser fornecidos com os seus interruptores. Caso não tenham sido enviados juntamente com os switches, você pode encomendá-los à NetApp (número de peça X1558A-R6).

Passos

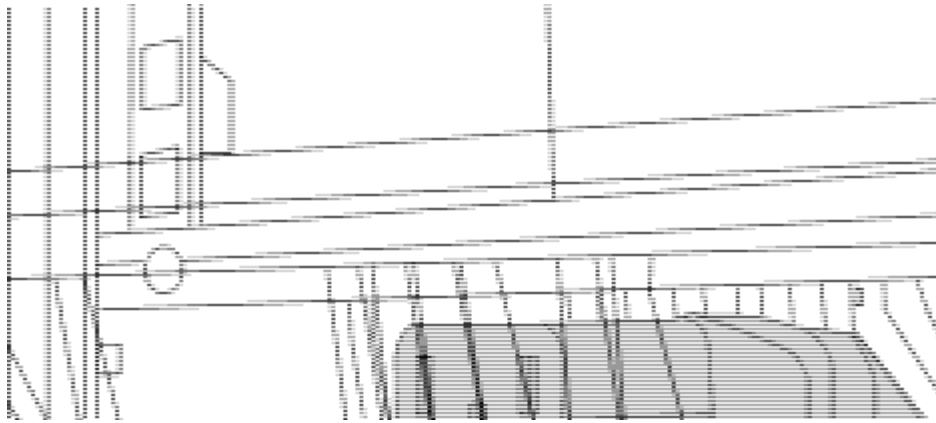
1. Instale o painel de vedação de passagem no gabinete NetApp .

O kit de painel de passagem está disponível na NetApp (número de peça X8784-R6).

O kit do painel de passagem da NetApp contém o seguinte hardware:

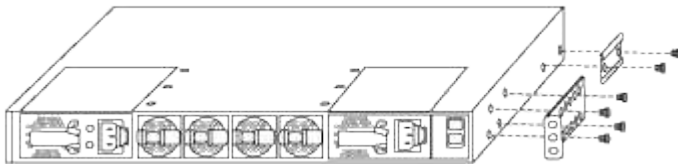
- Um painel de obturação de passagem
- Quatro parafusos 10-32 x 0,75
- Quatro porcas de clipe 10-32
 - i. Determine a localização vertical dos interruptores e do painel cego no gabinete.

Neste procedimento, o painel cego será instalado em U40.
 - ii. Instale duas porcas de clipe em cada lado nos furos quadrados apropriados para os trilhos frontais do gabinete.
 - iii. Centralize o painel verticalmente para evitar intrusão no espaço do rack adjacente e, em seguida, aperte os parafusos.
 - iv. Insira os conectores fêmea de ambos os cabos de ligação de 48 polegadas pela parte traseira do painel e através do conjunto da escova.

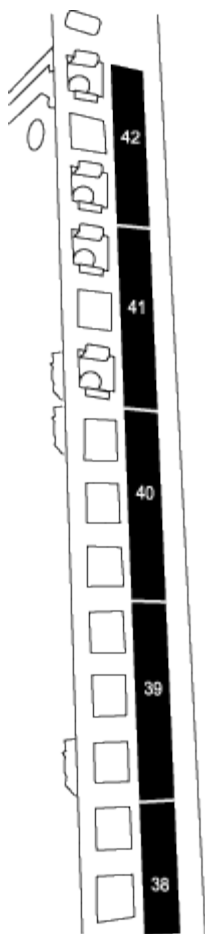


(1) Conector fêmea do cabo jumper.

1. Instale os suportes de montagem em rack no chassi do switch Nexus 92300YC.
 - a. Posicione um suporte de montagem em rack frontal em um lado do chassi do switch 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 fixar o suporte ao chassi.



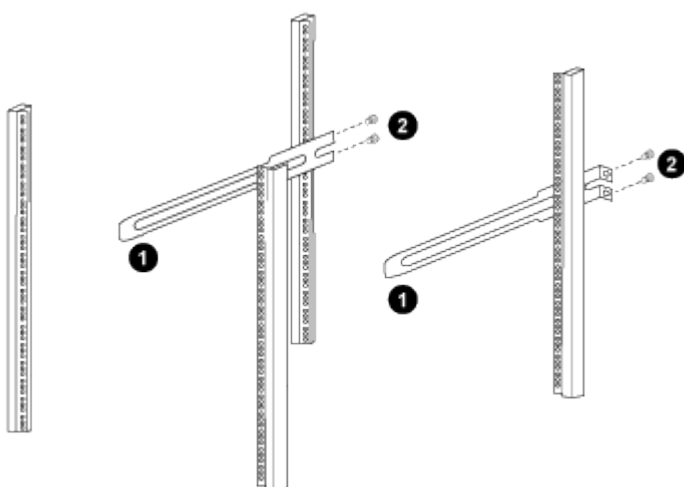
- b. Repita a etapa 2a com o outro suporte de montagem em rack frontal no outro lado do switch.
 - c. Instale o suporte de montagem em rack traseiro no chassi do switch.
 - d. Repita a etapa 2c com o outro suporte de montagem em rack traseiro no outro lado do switch.
2. Instale as porcas de clipe nos locais dos furos quadrados para todos 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 armário.

- a. Posicione o primeiro trilho deslizante na marca RU42 na parte traseira do poste traseiro esquerdo, insira os parafusos com a rosca correspondente e aperte-os 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 o poste traseiro do lado direito.

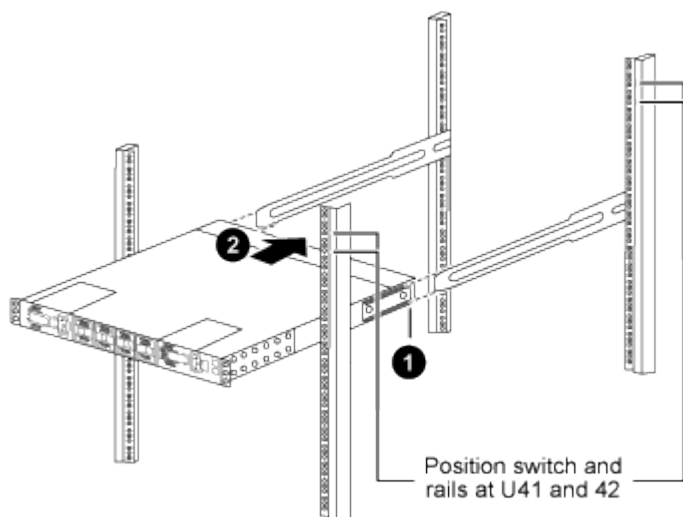
b. Repita os passos 4a e 4b nas localizações RU41 do gabinete.

4. Instale o interruptor no armário.



Esta etapa requer duas pessoas: uma para segurar o interruptor pela frente e outra para guiá-lo até os trilhos deslizantes traseiros.

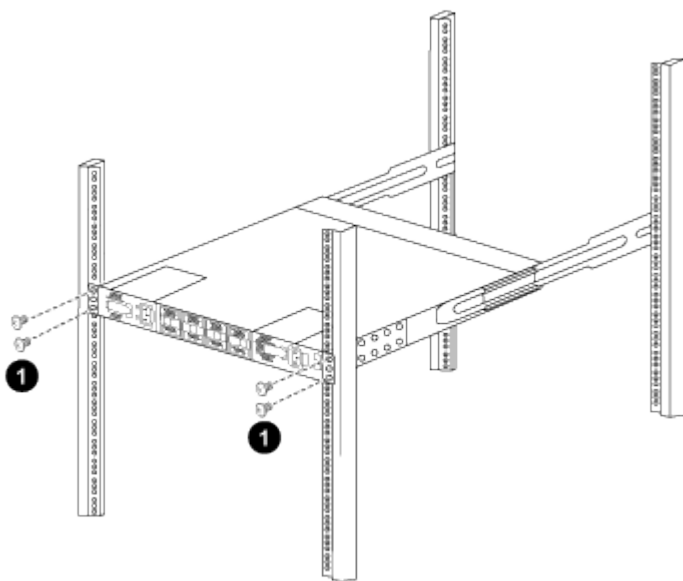
a. Posicione a parte traseira do interruptor em RU41.



(1) À medida que o chassi é empurrado em direção aos postes traseiros, alinhe as duas guias traseiras de montagem do rack com os trilhos deslizantes.

(2) Deslize suavemente o interruptor até que os suportes de montagem em rack frontais fiquem nivelados com os postes frontais.

b. Fixe o interruptor ao armário.



(1) Com uma pessoa segurando a parte frontal do chassi nivelada, a outra pessoa deve apertar completamente os quatro parafusos traseiros nos suportes do gabinete.

a. Com o chassi agora apoiado sem assistência, aperte completamente os parafusos dianteiros nos

postes.

b. Repita os passos 5a a 5c para o segundo interruptor na localização RU42.



Ao usar o switch totalmente instalado como suporte, não é necessário segurar a parte frontal do segundo switch durante o processo de instalação.

- Quando os interruptores estiverem instalados, conecte os cabos de ligação às entradas de energia dos interruptores.
- Conecte os plugues machos de ambos os cabos de ligação às tomadas PDU mais próximas disponíveis.



Para manter a redundância, os dois cabos devem ser conectados a PDUs diferentes.

- 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 roteado através do painel de passagem depois que os switches forem instalados para se conectar aos switches de gerenciamento ou à rede de gerenciamento.

O que vem a seguir

Após instalar os switches no gabinete NetApp , você pode ["configurar o switch"](#) .

Analise as considerações sobre cabeamento e configuração.

Antes de configurar seu switch Cisco 92300YC, revise as seguintes considerações.

Suporte para portas Ethernet NVIDIA CX6, CX6-DX e CX7.

Ao conectar uma porta de switch a um controlador ONTAP usando portas NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) ou ConnectX-7 (CX7), você deve definir a velocidade da porta do switch manualmente.

```
(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
```

Informações relacionadas

- Consulte o ["Hardware Universe"](#) para obter mais informações sobre portas de switch.
- Consulte ["Que informações adicionais preciso para instalar meu equipamento que não está no HWU?"](#) para obter mais informações sobre os requisitos de instalação 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 interruptor"

Configure 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 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 instalar e configurar o switch Cisco Nexus 92300YC.

Passos

1. Conecte a porta serial a um host ou a uma porta serial.
2. Conecte a porta de gerenciamento (no lado oposto às portas do switch) à mesma rede onde seu servidor SFTP está localizado.
3. No console, configure as definições seriais do lado do host:
 - 9600 baud
 - 8 bits de dados
 - 1 bit de parada
 - paridade: nenhuma
 - Controle de fluxo: nenhum
4. Ao ser inicializado pela primeira vez ou reiniciado após apagar a configuração em execução, o switch Nexus 92300YC entra em um loop de inicialização. Interrompa este ciclo digitando **sim** para abortar o

provisionamento automático de energia.

A configuração da conta de administrador do sistema é exibida.

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. Digite e confirme a senha do usuário administrador:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Digite **sim** 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. Configure as strings de comunidade SNMP de leitura e de leitura e gravação:

Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:

10. Configure o nome do switch do cluster:

Enter the switch name : **cs2**

11. Configure a interface de gerenciamento fora de 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 avançadas de IP:

```
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 switch e salve 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 vem a seguir?

Depois de configurar seus switches, você pode ["prepare-se para instalar o software NX-OS e RCF"](#).

Prepare-se para instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF).

Antes de instalar o software NX-OS e o Arquivo de Configuração de Referência (RCF), siga este procedimento.

Antes de começar

Certifique-se de ter o seguinte:

- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- O software apropriado e os guias de atualização estão disponíveis em ["Switches Cisco Nexus série 9000"](#).

Sobre os exemplos

Os exemplos neste procedimento usam dois nós. Esses nós usam duas portas de interconexão de cluster 10GbE e0a e e0b. Consulte a ["Hardware Universe"](#) para verificar as portas de cluster corretas em suas plataformas.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `node1` e `node2`.
- Os nomes LIF do cluster são `node1_clus1` e `node1_clus2` para o nó 1 e `node2_clus1` e `node2_clus2` para o nó 2.
- O `cluster1::*>` prompt indica o nome do cluster.

Sobre esta tarefa

O procedimento requer o uso de comandos ONTAP e comandos dos switches Cisco Nexus série 9000; os comandos ONTAP são usados a menos que indicado de outra forma. Os resultados dos comandos podem variar dependendo das diferentes versões do ONTAP.

Passos

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

```
set -privilege advanced
```

O prompt avançado(***>**) aparece.

2. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

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



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

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

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

3. Exibir quantas interfaces de interconexão de cluster estão 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 do cluster.
- Exibir os atributos da porta de rede: `network port show -ipspace Cluster`

Mostrar exemplo

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

```
Node: node2
```

Health					Speed (Mbps)	
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
```

Health					Speed (Mbps)	
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 do cluster remoto:

ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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: Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

Packet		Source	Destination
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			

Todas as versões do ONTAP

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

```
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. **[[passo 6]]** Verifique se o comando de reversão automática está habilitado 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
```

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

O que vem a seguir?

Após preparar a instalação do software NX-OS e do RCF, você pode ["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 a série MDS de switches de rede de área de armazenamento Fibre Channel (FC) fornecidos pela Cisco Systems.

Requisitos de revisão

Portas e conexões de nós suportadas

- Os links entre switches (ISLs) suportados para os switches Nexus 92300YC são as portas 1/65 e 1/66.
- As conexões de nó suportadas para os switches Nexus 92300YC são as portas 1/1 a 1/66.

Antes de começar

Certifique-se de ter o seguinte:

- O software NetApp Cisco NX-OS aplicável aos seus switches está disponível no site de suporte da NetApp . ["meusuporte.netapp.com"](#)
- Um cluster totalmente funcional (sem erros nos logs ou problemas semelhantes).
- ["Página do switch Ethernet da Cisco"](#). Consulte a tabela de compatibilidade de switches para obter informações sobre as versões suportadas do ONTAP e do NX-OS.

Instale o software

Os exemplos neste procedimento utilizam dois nós, mas você pode ter até 24 nós em um cluster.

Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 LIF do cluster são `node1_clus1` e `node1_clus2` para o nó 1 e `node2_clus1` e `node2_clus2` para o nó 2.
- O nome do espaço IP é `Cluster`.
- O `cluster1: :*>` O prompt indica o nome do cluster.
- As portas do cluster em cada nó são nomeadas. `e0a` e `e0b`.

Consulte a "[Hardware Universe](#)" para obter informações sobre as portas de cluster suportadas na sua plataforma. Consulte "[Que informações adicionais preciso para instalar meu equipamento que não está no HWU?](#)" para obter mais informações sobre os requisitos de instalação do switch.

Passos

1. Conecte o switch do cluster à rede de gerenciamento.
2. Use o `ping` Comando para verificar a conectividade com o servidor que hospeda o software NX-OS e o RCF.

Mostrar exemplo

Este exemplo verifica se o switch consegue 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 do software NX-OS em execução:

```
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 do NX-OS.

A instalação do arquivo de imagem faz com que ele seja carregado sempre que o switch for reiniciado.

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 após a reinicialização do switch:

```
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	IO FPGA	Successful

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 vem a seguir?

Após instalar o software NX-OS, você pode ["instalar o RCF"](#).

Instale o arquivo de configuração de referência (RCF)

Você pode instalar o RCF após configurar o switch Nexus 92300YC pela primeira vez. Você também pode usar este procedimento para atualizar sua versão do RCF.

Consulte o artigo da Knowledge Base ["Como limpar a configuração de um switch de interconexão Cisco mantendo a conectividade remota"](#) para obter mais informações ao instalar ou atualizar seu RCF.

Sobre esta tarefa

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches Cisco são `cs1` e `cs2`.
- Os nomes dos nós são `node1` e `node2`.
- Os nomes LIF do cluster são `node1_clus1`, `node1_clus2`, `node2_clus1`, e `node2_clus2`.
- O `cluster1::*>` O prompt indica o nome do cluster.



- O procedimento requer o uso de comandos ONTAP e ["Switches Cisco Nexus série 9000"](#). Os comandos ONTAP são usados a menos que indicado de outra forma.
- Antes de executar este procedimento, certifique-se de ter um backup atualizado da configuração do switch.
- Nenhum link operacional entre switches (ISL) é necessário durante este procedimento. Isso ocorre porque as alterações na versão do RCF podem afetar a conectividade ISL temporariamente. Para garantir a operação ininterrupta do cluster, o procedimento a seguir migra todas as LIFs do cluster para o switch parceiro operacional enquanto executa as etapas no switch de destino.

Passos

1. Exibir as portas do cluster em cada nó que estão conectadas 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
C92300YC      e0a     cs1                      Ethernet1/1/1      N9K-
C92300YC      e0b     cs2                      Ethernet1/1/1      N9K-
node2/cdp
C92300YC      e0a     cs1                      Ethernet1/1/2      N9K-
C92300YC      e0b     cs2                      Ethernet1/1/2      N9K-
cluster1::*>
```

2. Verifique o status administrativo e operacional de cada porta do cluster.

- a. Verifique se todas as portas do cluster estão ativas e com status íntegro:

```
network port show -ipSpace Cluster
```

Mostrar exemplo

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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 principal:
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
e0c      true      node1_clus1      up/up      169.254.3.4/23      node1
e0d      true      node1_clus2      up/up      169.254.3.5/23      node1
e0c      true      node2_clus1      up/up      169.254.3.8/23      node2
e0d      true      node2_clus2      up/up      169.254.3.9/23      node2
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: FOXXXXXXXXGS
 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: FOXXXXXXXXGD
 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, desligue as portas conectadas às portas de cluster dos nós.

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Verifique se as portas do cluster foram migradas 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 íntegro:

```
cluster show
```

### Mostrar exemplo

```
cluster1::*> *cluster show*
Node Health Eligibility Epsilon

node1 true true false
node2 true true false
cluster1::*>
```

### 7. Caso ainda não o tenha feito, 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 do switch CS2 e execute uma configuração básica.



Ao atualizar ou aplicar um novo RCF, você deve apagar as configurações do switch e realizar a configuração básica. Você deve estar conectado à porta serial do console do switch para configurá-lo 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 um reinício do switch:

#### Mostrar exemplo

```
(cs2)# reload

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

9. Copie o RCF para a bootflash do switch cs2 usando um dos seguintes protocolos de transferência: FTP, TFTP, SFTP ou SCP. Para mais informações sobre comandos da Cisco, consulte o guia apropriado na ["Switches Cisco Nexus série 9000"](#).

Este exemplo mostra o TFTP sendo usado para copiar um arquivo RCF para a memória 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 previamente baixado à memória flash de inicialização.

Para obter mais informações sobre os comandos da Cisco, consulte o guia apropriado em ["Switches Cisco Nexus série 9000"](#).

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 sucesso:

```
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
5HY9Kk3F9$YdCZ8iQJlRtoiEFa0sKP5IO/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 **ERRO: Falha ao gravar comandos VSH** é esperada e pode ser ignorada.

1. [[passo 12]]Verifique se o arquivo RCF é a versão mais recente correta:

```
show running-config
```

Ao verificar a saída para confirmar se você tem o RCF correto, certifique-se de que as seguintes informações estejam corretas:

- A bandeira da RCF
- Configurações de nó e porta
- Personalizações

O resultado varia de acordo com a configuração do seu site. Verifique as configurações da porta e consulte as notas de versão para quaisquer alterações específicas do RCF que você instalou.

2. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração](#)." Para obter detalhes sobre quaisquer alterações adicionais necessárias.
3. Após 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 os comandos da Cisco, consulte o guia apropriado em "[Switches Cisco Nexus série 9000](#)".

```
cs2# copy running-config startup-config
[] 100% Copy complete
```

4. Reinicie o switch cs2. Você pode ignorar os eventos "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs2# reload
This command will reboot the system. (y/n)? [n] y
```

5. Verifique a integridade das portas do cluster.
  - a. Verifique se as portas e0d estão ativas e íntegras em todos os nós do cluster:  

```
network port show -ip space Cluster
```

## Mostrar exemplo

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

Node: node1

Ignore

Health Health Speed (Mbps)
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

Health Health Speed (Mbps)
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 o estado de saúde do switch no cluster (isso pode não mostrar o switch cs2, já que as LIFs não estão configuradas 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: FOXXXXXXXXGD
 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: FOXXXXXXXXGS
 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 poderá observar a seguinte saída no console do switch cs1, dependendo da versão do 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, desligue as portas conectadas às portas de cluster dos nós.

O exemplo a seguir utiliza a saída de exemplo da interface da etapa 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

7. Verifique se as LIFs do cluster foram migradas 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 íntegro:

```
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 switch cs1.

10. Ative a reversão automática nos LIFs do cluster.

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

11. Reinicie o interruptor cs1. Você faz isso para que as LIFs do cluster voltem às suas portas originais. Você pode ignorar os eventos "portas do cluster inativas" relatados nos nós enquanto o switch reinicia.

```
cs1# reload
This command will reboot the system. (y/n)? [n] y
```

12. Verifique se as portas do switch conectadas às portas do cluster estão ativas.

```
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 a ISL entre cs1 e cs2 está funcionando:

```
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 as LIFs do cluster retornaram à sua porta original:

```
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 íntegro:

```
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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| Loss                     |             |             |
| -----                    | -----       | -----       |
| node1                    |             |             |
| 3/5/2022 19:21:18 -06:00 | node1_clus2 | node2-clus1 |
| node2                    |             |             |
| 3/5/2022 19:21:20 -06:00 | node1_clus2 | node2_clus2 |
| node1                    |             |             |
| 3/5/2022 19:21:18 -06:00 | node2_clus2 | node1_clus1 |
| node2                    |             |             |
| 3/5/2022 19:21:20 -06:00 | node2_clus2 | node1_clus2 |

## Todas as versões do ONTAP

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

```
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 vem a seguir?

Após instalar o RCF, você pode ["verificar a configuração SSH"](#).

### Verifique sua configuração SSH.

Se você estiver usando o Monitor de Saúde do Switch Ethernet (CSHM) e os recursos de coleta de logs, verifique se o SSH e as chaves SSH estão habilitados nos switches do 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
AAAAB3NzaC1yc2EAAAADAQABAAQgQDiNrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
17nwlIoC6HBejxluIObAH8hrW8kR+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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIAbm1zdHA1MjEAAACFBABJ+ZX5SFKhS57e
vke273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVliewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
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 habilitar o FIPS, você deve alterar a contagem de bits para 256 no switch usando o comando `ssh key ecdsa 256 force`. Consulte ["Configure a segurança de rede usando FIPS."](#) para mais detalhes.

### O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar monitoramento de integridade do switch"](#).

## Migrar switches

### Migre para um cluster comutado de dois nós com um switch Cisco Nexus 92300YC.

Se você já possui um ambiente de cluster de dois nós sem switches, pode migrar para um ambiente de cluster de dois nós com switches, utilizando switches Cisco Nexus 92300YC, o que permite escalar o cluster para além de dois nós.

O procedimento a ser utilizado depende de você ter 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 utilizam portas ópticas ou twinax, mas não é suportado neste switch se os nós estiverem utilizando portas RJ45 10Gb BASE-T integradas para as portas de rede do cluster.

A maioria dos sistemas requer duas portas de rede dedicadas para clusters 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. Consulte ["Monitoramento de saúde do switch \(CSHM\)"](#).

### Requisitos de revisão

#### Antes de começar

Certifique-se de ter o seguinte:

Para uma configuração sem switch de dois nós, certifique-se de que:

- A configuração sem switch de dois nós está configurada corretamente e funcionando.
- Os nós estão executando o ONTAP 9.6 ou posterior.
- Todas as portas do cluster estão no estado **ativo**.
- Todas as interfaces lógicas do cluster (LIFs) estão no estado **ativo** e em suas portas de origem.

Para a configuração do switch Cisco Nexus 92300YC:

- Ambos os switches possuem conectividade de rede de gerenciamento.
- É possível acessar os switches do cluster através do console.
- As conexões entre nós e entre switches do Nexus 92300YC utilizam cabos twinax ou de fibra óptica.

O ["Hardware Universe - Switches"](#) contém mais informações sobre cabeamento.

- Os cabos Inter-Switch Link (ISL) são conectados às portas 1/65 e 1/66 em ambos os switches 92300YC.
- A personalização inicial de ambos os switches 92300YC foi concluída. Para que:
  - Os switches 92300YC estão executando a versão mais recente do software.

- Os arquivos de configuração de referência (RCFs) são aplicados aos switches. Qualquer personalização do site, como SMTP, SNMP e SSH, é configurada nos novos switches.

## Migre o switch

### Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- 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, respectivamente.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas do cluster utilizadas neste procedimento são e0a e e0b.

O "[Hardware Universe](#)" contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

## Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado(`*>`) aparece.

2. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

onde x representa a duração do período de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

### Mostrar exemplo

O comando a seguir suprima 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 os nós (exceto as portas ISL) nos dois novos switches do cluster, cs1 e cs2.

Você não deve desativar as portas ISL.

#### Mostrar exemplo

O exemplo a seguir mostra que as portas voltadas para o nó, de 1 a 64, 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 ativos nas portas 1/65 e 1/66:

```
show port-channel summary
```

## Mostrar exemplo

O exemplo a seguir mostra que as portas ISL estão ativas no switch 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 ativas no switch 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 Eth1/65 (P) Eth1/66 (P)
```



3. Exibir a lista de dispositivos vizinhos:

```
show cdp neighbors
```

Este comando fornece informações sobre os dispositivos que estão conectados 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:

+

```
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 aparecer para cima. Link e saudável para Health Status .

### Mostrar exemplo

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

Node: node1

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

Node: node2

| Port | IPspace | Broadcast Domain | Link | MTU  | Speed(Mbps)<br>Admin/Oper | Health<br>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 do cluster estão ativas e operacionais:

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

Cada LIF de cluster deve exibir verdadeiro para Is Home e tenha um Status Admin/Oper de cima/para cima

### 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. Desative a reversão automática em todas as 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 entries were displayed. |             |             |

7. Desconecte o cabo da porta do cluster e0a no nó 1 e, em seguida, conecte e0a à porta 1 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches 92300YC.

O "[Hardware Universe - Switches](#)" contém mais informações sobre cabeamento.

- Desconecte o cabo da porta do cluster e0a no nó 2 e, em seguida, conecte e0a à porta 2 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches 92300YC.
- Habilite todas as portas voltadas para os nós no switch de cluster cs1.

#### Mostrar exemplo

O exemplo a seguir mostra que as portas 1/1 a 1/64 estão habilitadas 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
```

- 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 todas as LIFs estão ativas no nó 1 e no nó 2 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 estado 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.
```

- Desconecte o cabo da porta do cluster e0b no nó 1 e, em seguida, conecte e0b à porta 1 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches 92300YC.
- Desconecte o cabo da porta do cluster e0b no nó 2 e, em seguida, conecte e0b à porta 2 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches 92300YC.
- Habilite todas as portas voltadas para os nós no switch de cluster cs2.

**Mostrar exemplo**

O exemplo a seguir mostra que as portas 1/1 a 1/64 estão habilitadas 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**

- Ative a reversão automática nos LIFs do cluster.

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

- 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 ativas no nó 1 e no nó 2:

```
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.

### 3. Verifique se todas as interfaces exibem verdadeiro para Is Home :

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



Isso pode levar alguns minutos para ser concluído.

### Mostrar exemplo

O exemplo a seguir mostra que todas as LIFs estão ativas no nó 1 e no nó 2 e que Is Home Os resultados são verdadeiros:

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

| Current Is | Logical     | Status     | Network           | Current |      |
|------------|-------------|------------|-------------------|---------|------|
| Vserver    | Interface   | Admin/Oper | Address/Mask      | Node    | Port |
| Home       |             |            |                   |         |      |
| -----      | -----       | -----      | -----             | -----   |      |
| -----      | ----        |            |                   |         |      |
| Cluster    |             |            |                   |         |      |
| true       | 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.

4. Verifique se ambos os nós possuem uma conexão com cada switch:

```
show cdp neighbors
```



**Mostrar exemplo**

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
(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<br>Port ID        | Local Intrfce | Hldtme | Capability | Platform     |
|-----------------------------|---------------|--------|------------|--------------|
| node1<br>e0a                | Eth1/1        | 133    | H          | FAS2980      |
| node2<br>e0a                | Eth1/2        | 133    | H          | FAS2980      |
| cs2(FDO220329V5)<br>Eth1/65 | Eth1/65       | 175    | R S I s    | N9K-C92300YC |
| cs2(FDO220329V5)<br>Eth1/66 | Eth1/66       | 175    | R S I s    | N9K-C92300YC |

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<br>Port ID        | Local Intrfce | Hldtme | Capability | Platform     |
|-----------------------------|---------------|--------|------------|--------------|
| node1<br>e0b                | Eth1/1        | 133    | H          | FAS2980      |
| node2<br>e0b                | Eth1/2        | 133    | H          | FAS2980      |
| cs1(FDO220329KU)<br>Eth1/65 | Eth1/65       | 175    | R S I s    | N9K-C92300YC |
| cs1(FDO220329KU)<br>Eth1/66 | Eth1/66       | 175    | R S I s    | N9K-C92300YC |

Total entries displayed: 4

5. Exibir 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
 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.
```

6. Verifique se as configurações estão desativadas:

```
network options switchless-cluster show
```



A conclusão do comando pode levar alguns minutos. Aguarde o anúncio de que o tempo de vida de 3 minutos está prestes a expirar.

**Mostrar exemplo**

O resultado incorreto 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 nós membros do cluster:

```
cluster show
```

### Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. [[passo 8]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do 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 administrador:

```
set -privilege admin
```

#### O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar monitoramento de integridade do switch"](#).

## Substitua os interruptores

### Substituir um switch Cisco Nexus 92300YC

A substituição de um switch Nexus 92300YC defeituoso em uma rede cluster é um procedimento não disruptivo (NDU).

#### Requisitos de revisão

#### Antes de começar

Antes de substituir o interruptor, certifique-se de que:

- Na infraestrutura de cluster e rede existente:
  - O cluster existente foi verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
  - Todas as portas do cluster estão ativas.
  - Todas as interfaces lógicas do cluster (LIFs) estão ativas e em suas portas de origem.
  - O comando `ping-cluster -node node1` do cluster ONTAP deve indicar que a conectividade básica e a comunicação com largura de banda superior a PMTU estão funcionando corretamente em todos os caminhos.
- Para o switch de substituição do Nexus 92300YC:
  - A conectividade da rede de gerenciamento no switch de substituição está funcionando corretamente.
  - O acesso ao console do interruptor de substituição já está instalado.
  - As conexões do nó são as portas 1/1 a 1/64.
  - Todas as portas de Interconexão de Switches (ISL) estão desativadas nas portas 1/65 e 1/66.
  - O arquivo de configuração de referência (RCF) desejado e a imagem do sistema operacional NX-OS são carregados no switch.
  - A personalização inicial do interruptor está concluída, conforme detalhado em: ["Configure o switch Cisco Nexus 92300YC."](#)

Quaisquer personalizações anteriores do site, como STP, SNMP e SSH, são copiadas para o novo switch.

#### Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

## **Substitua o interruptor**

### **Sobre os exemplos**

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor 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 do cluster em cada nó são denominadas e0a e e0b.
- Os nomes 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 para alterações em todos os nós do cluster é cluster1::\*>

### **Sobre esta tarefa**

Você deve executar o comando para migrar um LIF de cluster a partir do nó onde o LIF de cluster está hospedado.

O procedimento a seguir baseia-se na seguinte topologia de rede em 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 (FD0220329V5) | Eth1/65       | 176    | R S I s    | N9K-C92300YC |      |
| Eth1/65           |               |        |            |              |      |
| cs2 (FD0220329V5) | 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<br>ID   | Local Intrfce | Hldtme | Capability | Platform     | Port |
|-------------------|---------------|--------|------------|--------------|------|
| 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

## Etapa 1: Prepare-se para a substituição

1. Instale o RCF e a imagem apropriados no switch, newcs2, e faça todos os preparativos necessários no local.

Caso necessário, verifique, baixe e instale as versões apropriadas dos softwares RCF e NX-OS para o novo switch. Se você verificou que o novo switch está configurado corretamente e não precisa de atualizações nos softwares RCF e NX-OS, continue para a etapa 2.

- a. Acesse a página *NetApp Cluster and Management Network Switches Reference Configuration File Description* no site de suporte da NetApp .
  - b. Clique no link para a *Matriz de Compatibilidade de Rede de Cluster e Rede de Gerenciamento* e, em seguida, observe a versão de software do switch necessária.
  - c. Clique na seta "Voltar" do seu navegador para retornar à página de **Descrição**, clique em **CONTINUAR**, aceite o contrato de licença e, em seguida, acesse a página de **Download**.
  - d. Siga os passos na página de Download para baixar os arquivos RCF e NX-OS corretos para a versão do software ONTAP que você está instalando.
2. No novo switch, efetue login como administrador e desligue todas as portas que serão conectadas às interfaces do cluster de nós (portas 1/1 a 1/64).

Se o interruptor que você está substituindo não estiver funcionando e estiver desligado, vá para a Etapa 4. As LIFs nos nós do cluster já devem ter migrado para a outra porta do cluster em 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
```

| Vserver | Logical 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. Desative 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 conecte-os às mesmas portas no switch Nexus 92300YC newcs2.
3. Abra as portas ISLs 1/65 e 1/66 entre os switches cs1 e newcs2 e, em seguida, verifique o status da operação do canal da porta.

Port-Channel deve indicar Po1(SU) e Member Ports deve indicar Eth1/65(P) e Eth1/66(P).

## Mostrar exemplo

Este exemplo habilita as portas ISL 1/65 e 1/66 e exibe o resumo do canal de porta no switch 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

O resultado deverá ser semelhante ao seguinte:

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

Node: node1

Ignore

Health Health Speed (Mbps)
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

Health Health Speed (Mbps)
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 a LIF do cluster associada à porta da etapa anterior usando o comando `network interface revert`.



### Mostrar exemplo

Neste exemplo, a LIF `node1_clus2` no nó 1 é revertida com sucesso se o valor de `Home` for verdadeiro e a porta for `e0b`.

Os seguintes comandos retornam LIF `node1_clus2` sobre `node1` para o porto de origem `e0a` e exibe informações sobre os LIFs em ambos os nós. A inicialização do primeiro nó é bem-sucedida se a coluna "Is Home" (É o nó principal) for verdadeira para ambas as interfaces do cluster e elas mostrarem as atribuições de porta corretas, neste exemplo. `e0a` e `e0b` no nó 1.

```
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 o estado de saúde dos nós `node1` e `node2` neste cluster é verdadeiro:

```
cluster1::*> cluster show
```

| Node  | Health | Eligibility |
|-------|--------|-------------|
| ----- | -----  | -----       |
| node1 | false  | true        |
| node2 | true   | true        |

## 7. Verifique se todas as portas físicas do cluster estão ativas:

```
network port show ipspace Cluster
```

### Mostrar exemplo

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

Node: node1

Ignore

| Health  | Health  |           |        |       |       | Speed (Mbps) |
|---------|---------|-----------|--------|-------|-------|--------------|
| 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

| Health  | Health  |           |        |       |       | Speed (Mbps) |
|---------|---------|-----------|--------|-------|-------|--------------|
| 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: Conclua o procedimento

### 1. Verifique a conectividade das interfaces do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. **[[passo 2]]** Confirme a seguinte configuração de rede do 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<br>Port ID         | Local Intrfce | Hldtme | Capability | Platform     |
|------------------------------|---------------|--------|------------|--------------|
| node1<br>e0b                 | Eth1/1        | 139    | H          | FAS2980      |
| node2<br>e0b                 | Eth1/2        | 124    | H          | FAS2980      |
| cs1 (FDO220329KU)<br>Eth1/65 | Eth1/65       | 178    | R S I s    | N9K-C92300YC |
| cs1 (FDO220329KU)<br>Eth1/66 | Eth1/66       | 178    | R S I s    | N9K-C92300YC |

```
Total entries displayed: 4
```

### O que vem a seguir?

Após verificar sua configuração SSH, você pode ["configurar monitoramento de integridade do switch"](#).

### Substituir switches de cluster Cisco Nexus 92300YC por conexões sem switch

É possível migrar de um cluster com uma rede de cluster comutada para uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

#### Requisitos de revisão

#### Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está

executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

### Antes de começar

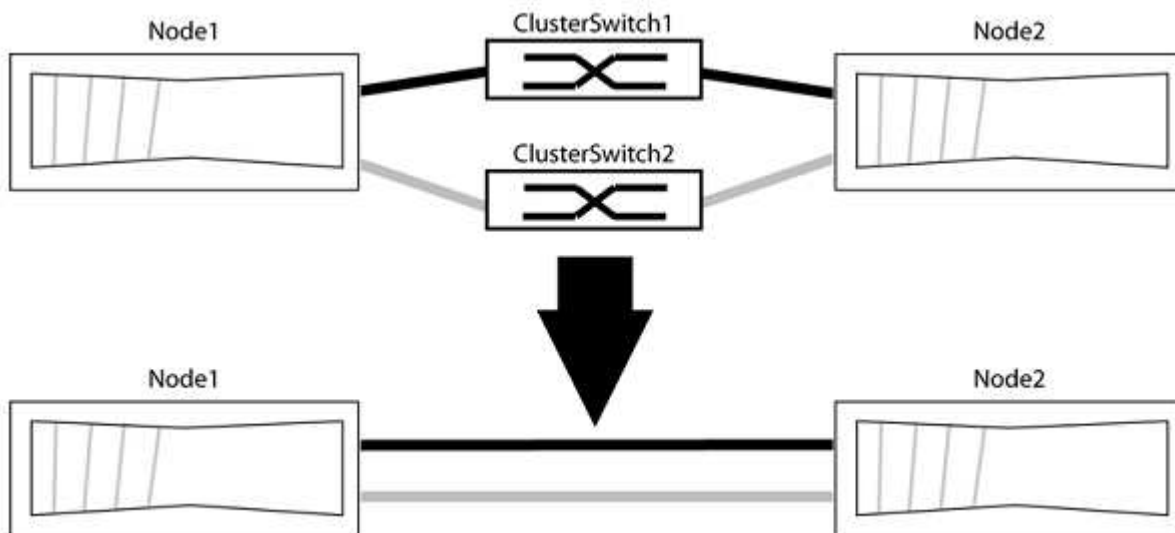
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

### Migre 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 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 elas variam de acordo com o sistema.

### Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:



```
network options detect-switchless-cluster show
```

### Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

onde `h` é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

### Mostrar exemplo

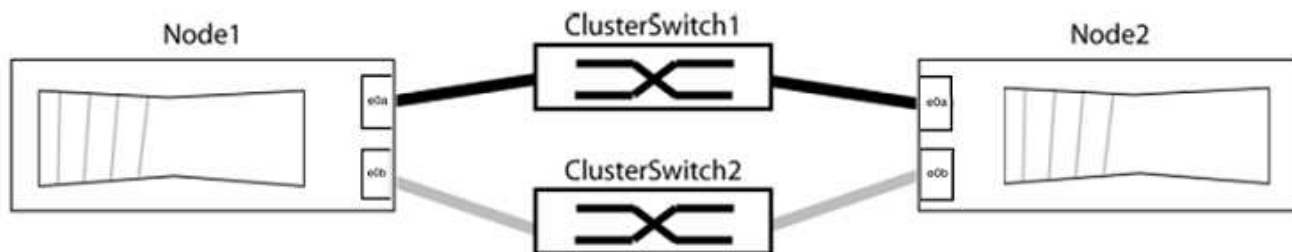
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

## Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de up para a coluna “Link” e um valor de healthy para a coluna “Estado de Saúde”.

### 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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está true para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

### Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

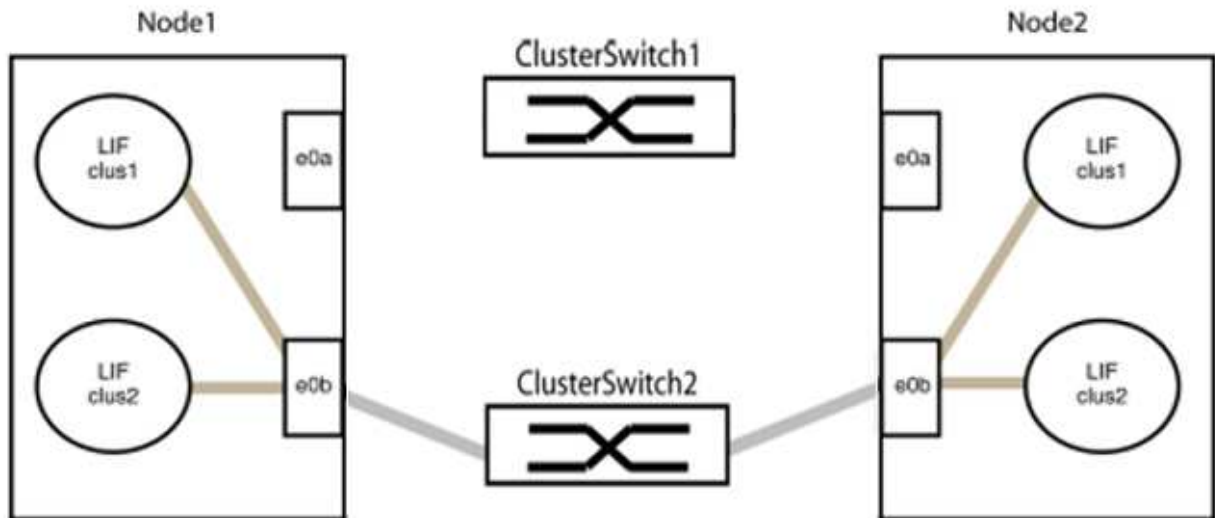
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

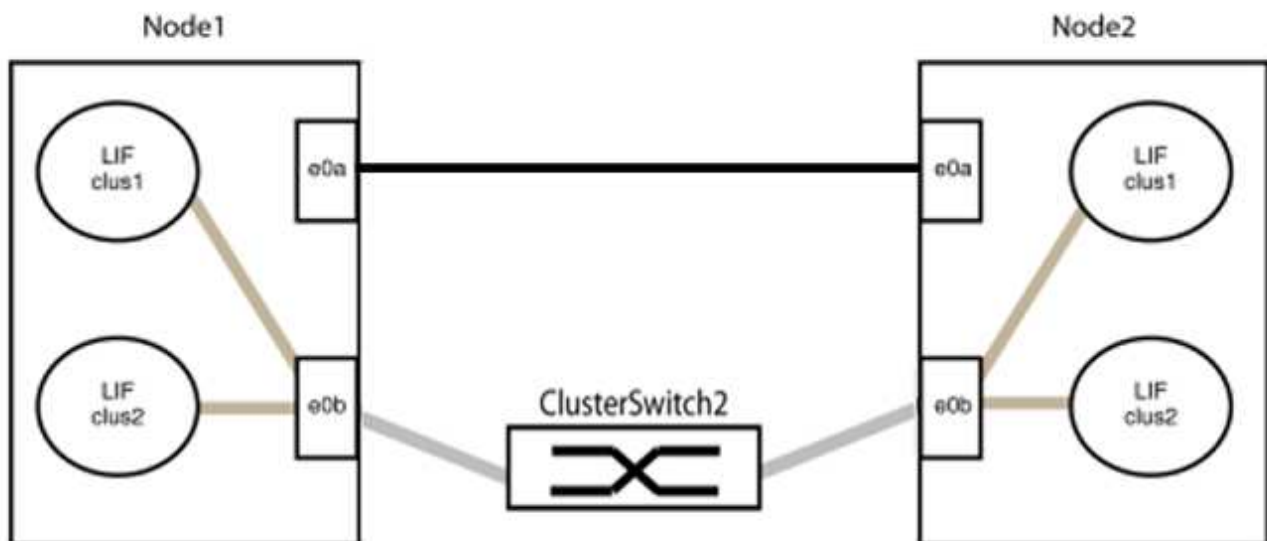
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

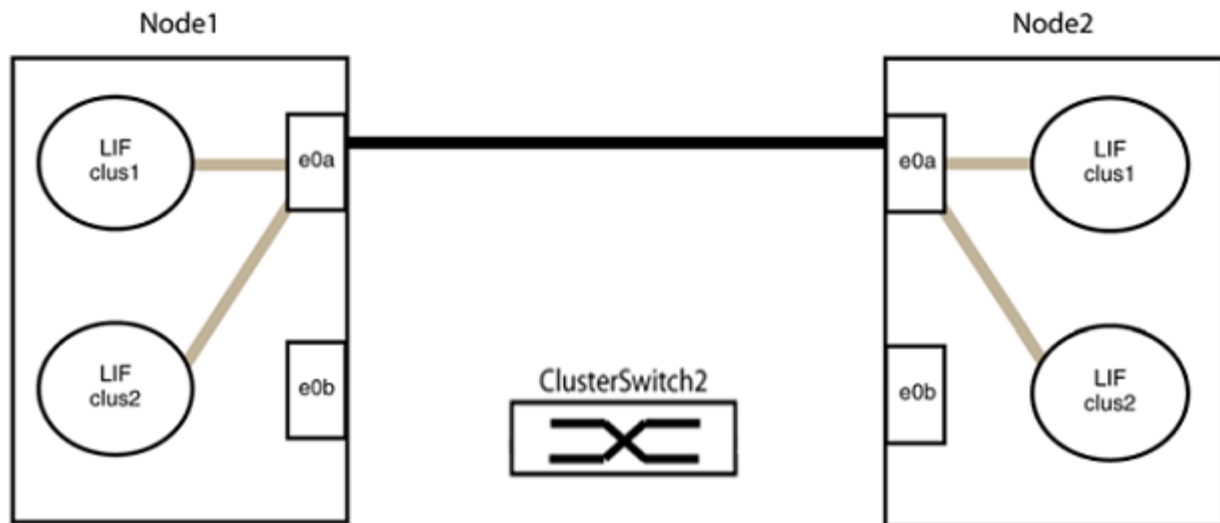
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

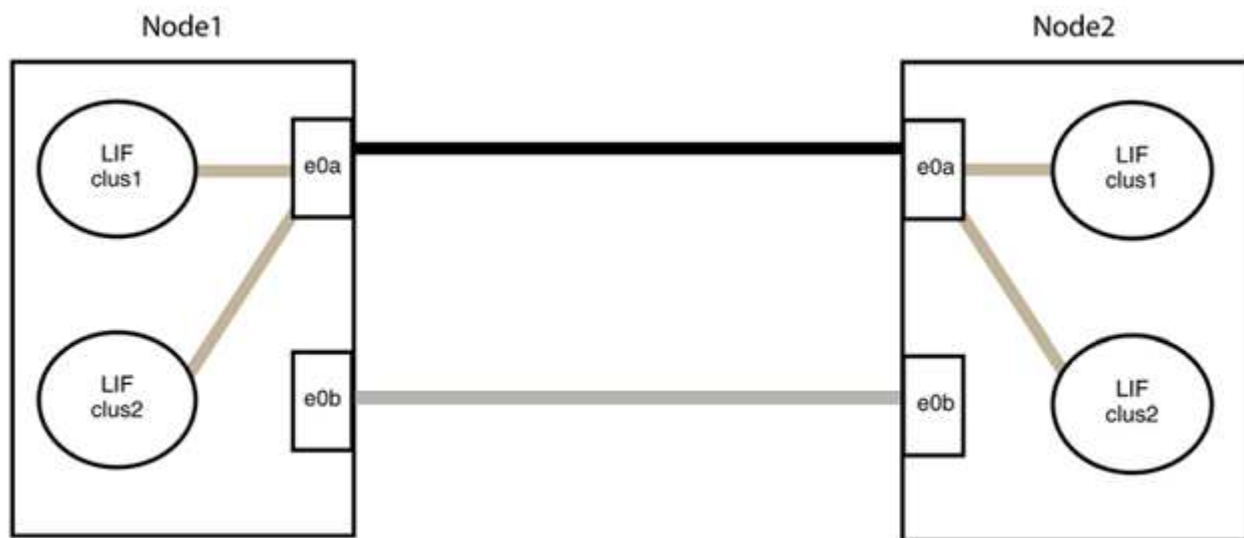
- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



### Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

## Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna “Is Home” estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

### Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node Health Eligibility Epsilon

node1 true true false
node2 true true false
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. [[passo 6]] Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

## NetApp CN1610

### Visão geral da instalação e configuração dos switches NetApp CN1610

O CN1610 é um switch gerenciável de camada 2 de alta largura de banda que fornece 16 portas SFP+ (Small Form-Factor Pluggable Plus) de 10 Gigabits.

O switch inclui fontes de alimentação redundantes e bandejas de ventoinhas que suportam a troca a quente para alta disponibilidade. Este switch de 1U pode ser instalado em um gabinete de sistema NetApp 42U

padrão de 19 polegadas ou em um gabinete de terceiros.

O switch suporta gerenciamento local através da porta de console ou gerenciamento remoto usando Telnet ou SSH por meio de uma conexão de rede. O CN1610 inclui uma porta de gerenciamento RJ45 dedicada de 1 Gigabit Ethernet para gerenciamento de switch fora de banda. Você pode gerenciar o switch inserindo comandos na interface de linha de comando (CLI) ou usando um sistema de gerenciamento de rede (NMS) baseado em SNMP.

## Instalar e configurar o fluxo de trabalho para switches NetApp CN1610.

Para instalar e configurar um switch NetApp CN1610 em sistemas que executam o ONTAP, siga estas etapas:

1. ["Instalar hardware"](#)
2. ["Instale o software FASTPATH"](#)
3. ["Instale o arquivo de configuração de referência."](#)

Se os switches estiverem executando o ONTAP 8.3.1 ou posterior, siga as instruções em ["Instale o FASTPATH e os RCFs em switches que executam o ONTAP 8.3.1 ou posterior."](#)

4. ["Configurar interruptor"](#)

## Requisitos de documentação para switches NetApp CN1610

Para a instalação do switch NetApp CN1610, certifique-se de revisar toda a documentação recomendada.

| Título do documento                                                              | Descrição                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">"Guia de Instalação 1G"</a>                                          | Uma visão geral das características de hardware e software do switch CN1601 e do processo de instalação.                                                                                                                                                                                      |
| <a href="#">"Guia de Instalação 10G"</a>                                         | Uma visão geral dos recursos de hardware e software do switch CN1610, incluindo instruções sobre como instalar o switch e acessar a CLI.                                                                                                                                                      |
| <a href="#">"Guia de Instalação e Configuração dos Switches CN1601 e CN1610"</a> | Detalhes sobre como configurar o hardware e o software do switch para o seu ambiente de cluster.                                                                                                                                                                                              |
| Guia do Administrador do Switch CN1601                                           | Fornece exemplos de como usar o switch CN1601 em uma rede típica. <ul style="list-style-type: none"><li>• <a href="#">"Guia do Administrador"</a></li><li>• <a href="#">"Guia do Administrador, Versão 1.1.xx"</a></li><li>• <a href="#">"Guia do Administrador, Versão 1.2.xx"</a></li></ul> |

| Título do documento                                    | Descrição                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Referência de comandos da CLI do switch de rede CN1610 | <p>Fornecer informações detalhadas sobre os comandos da interface de linha de comando (CLI) que você usa para configurar o software CN1601.</p> <ul style="list-style-type: none"> <li>• <a href="#">"Referência de comandos"</a></li> <li>• <a href="#">"Referência de comandos, versão 1.1.xx"</a></li> <li>• <a href="#">"Guia de Comandos, Versão 1.2.xx"</a></li> </ul> |

## Instalar e configurar

### Instale o hardware para o switch NetApp CN1610.

Para instalar o hardware do switch NetApp CN1610, utilize as instruções em um dos seguintes guias.

- ["Guia de Instalação 1G"](#).

Uma visão geral das características de hardware e software do switch CN1601 e do processo de instalação.

- ["Guia de Instalação 10G"](#)

Uma visão geral dos recursos de hardware e software do switch CN1610, incluindo instruções sobre como instalar o switch e acessar a CLI.

### Instale o software FASTPATH

Ao instalar o software FASTPATH em seus switches NetApp, você deve iniciar a atualização pelo segundo switch, cs2.

#### Requisitos de revisão

##### Antes de começar

Certifique-se de ter o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster estão configuradas.
- Todas as interfaces lógicas do cluster (LIFs) devem estar configuradas (não devem ter sido migradas).
- Um caminho de comunicação bem-sucedido: O ONTAP (privilegio: avançado) `cluster ping-cluster -node node1` O comando deve indicar que `larger than PMTU communication` Tem sucesso em todos os caminhos.
- Uma versão compatível do FASTPATH e do ONTAP.



Certifique-se de consultar a tabela de compatibilidade de switches no "[Switches NetApp CN1601 e CN1610](#)" Página com as versões suportadas do FASTPATH e do ONTAP .

## Instale o FASTPATH

O procedimento a seguir utiliza a sintaxe clusterizada do Data ONTAP 8.2. Como resultado, o Vserver do cluster, os nomes LIF e a saída da CLI são diferentes daqueles presentes no Data ONTAP 8.3.

Pode haver dependências entre a sintaxe de comandos nas versões RCF e FASTPATH.

## Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os dois switches NetApp são o cs1 e o cs2.
- Os dois LIFs do cluster são clus1 e clus2.
- Os servidores virtuais são vs1 e vs2.
- O `cluster: *` O prompt indica o nome do cluster.
- As portas do cluster em cada nó são denominadas e1a e e2a.

O "[Hardware Universe](#)" contém mais informações sobre as portas de cluster reais que são suportadas em sua plataforma.

- Os links entre switches (ISLs) suportados são as portas 0/13 a 0/16.
- As conexões de nó suportadas são as portas 0/1 a 0/12.

## Etapa 1: Migrar cluster

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

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

2. Faça login no switch como administrador. Não há senha por padrão. No (cs2) # conforme solicitado, 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 o 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
```

| Vserver | Logical Interface | Status Admin/Open | Network Address/Mask | Current Node | Current Port | Is 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   |                   |                   |                      |              |              |         |

**Etapa 2: Instale o software FASTPATH**

1. Desative a porta e2a do cluster em ambos os nós:

```
network port modify
```

### Mostrar exemplo

O exemplo a seguir mostra a porta e2a sendo desativada 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 desativada em ambos os nós:

```
network port show
```

### Mostrar exemplo

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

| (Mbps) |      |         |      |       | Auto-Negot | Duplex     | Speed      |
|--------|------|---------|------|-------|------------|------------|------------|
| 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. Desative as portas Inter-Switch Link (ISL) no cs1, o switch 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 backup 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. Faça o download do arquivo de imagem para o switch.

Copiar o arquivo de imagem para a imagem ativa significa que, ao reiniciar, essa imagem estabelece a versão do FASTPATH em execução. A imagem anterior permanece disponível como backup.

### 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 inicialização para a configuração ativa e de backup.

```
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!
```

### Etapa 3: Validar 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. Ative as portas ISL no cs1, o switch 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 Link State deve indicar Up .



### 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 salve o arquivo quando estiver satisfeito com as versões do software e as configurações do 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
```

A 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 agora está em casa.(true ) em ambos os nós:

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

### Mostrar exemplo

```
cluster::*> network interface show -role cluster
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is 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. Veja o estado dos nós:

```
cluster show
```

## Mostrar exemplo

```
cluster::> cluster show
```

| Node  | Health | Eligibility |
|-------|--------|-------------|
| node1 | true   | true        |
| node2 | true   | true        |

9. Repita os passos anteriores para instalar o software FASTPATH no outro switch, cs1.

10. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do AutoSupport :

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

## Instale um arquivo de configuração de referência em um switch CN1610.

Siga este procedimento para instalar um Arquivo de Configuração de Referência (RCF).

Antes de instalar um RCF, você deve primeiro migrar as LIFs do cluster do switch cs2. Após a instalação e validação do RCF, os LIFs podem ser migrados de volta.

### Requisitos de revisão

#### Antes de começar

Certifique-se de ter o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster estão configuradas.
- Todas as interfaces lógicas do cluster (LIFs) estão configuradas.
- Um caminho de comunicação bem-sucedido: O ONTAP (privilegio: avançado) `cluster ping-cluster -node node1` O comando deve indicar que `larger than PMTU communication` Tem sucesso em todos os caminhos.
- Uma versão compatível do RCF e do ONTAP.

Certifique-se de consultar a tabela de compatibilidade de switches no ["Switches NetApp CN1601 e CN1610"](#) Página com as versões RCF e ONTAP suportadas.

### Instale o RCF

O procedimento a seguir utiliza a sintaxe clusterizada do Data ONTAP 8.2. Como resultado, o Vserver do cluster, os nomes LIF e a saída da CLI são diferentes daqueles presentes no Data ONTAP 8.3.

Pode haver dependências entre a sintaxe de comandos nas versões RCF e FASTPATH.



Na versão 1.2 do RCF, o suporte para Telnet foi explicitamente desativado devido a preocupações de segurança. Para evitar problemas de conectividade durante a instalação do RCF 1.2, verifique se o Secure Shell (SSH) está ativado. O ["Guia do Administrador do Switch NetApp CN1610"](#) Possui mais informações sobre SSH.

## Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os dois switches NetApp são o cs1 e o cs2.
- Os dois LIFs do cluster são clus1 e clus2.
- Os servidores virtuais são vs1 e vs2.
- O `cluster::*>` O prompt indica o nome do cluster.
- As portas do cluster em cada nó são denominadas e1a e e2a.

O ["Hardware Universe"](#) contém mais informações sobre as portas de cluster reais que são suportadas em sua plataforma.

- Os links entre switches (ISLs) suportados são as portas 0/13 a 0/16.
- As conexões de nó suportadas são as portas 0/1 a 0/12.
- Uma versão compatível de FASTPATH, RCF e ONTAP.

Certifique-se de consultar a tabela de compatibilidade de switches no ["Switches NetApp CN1601 e CN1610"](#) Página com as versões suportadas de FASTPATH, RCF e ONTAP .

## Etapa 1: Migrar cluster

1. Salve as informações de configuração atuais do seu switch:

```
write memory
```

### Mostrar exemplo

O exemplo a seguir mostra a configuração atual do switch sendo salva na configuração de inicialização.(`startup-config`) arquivo 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 o 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. Desative a porta e2a em ambos os nós:

```
network port modify
```

#### Mostrar exemplo

O exemplo a seguir mostra a porta e2a sendo desativada 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 desativada em ambos os nós:

```
network port show
```

### Mostrar exemplo

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

| (Mbps) |       |         |      |       | Auto-Negot | Duplex     | Speed      |
|--------|-------|---------|------|-------|------------|------------|------------|
| 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 switch 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
```

## Etapa 2: Instalar o RCF

1. Copie o RCF para o switch.



Você deve definir o `.scr` A extensão deve fazer parte do nome do arquivo antes de executar o script. Esta extensão é para o sistema operacional FASTPATH.

O switch validará o script automaticamente à medida que ele for baixado para o switch, e a saída será exibida no 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 de arquivo que você definiu.

### 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 interruptor.

#### 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 as alterações foram implementadas no switch.

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

O exemplo exibe o `running-config` arquivo no interruptor. Você deve comparar o arquivo com o RCF para verificar se os parâmetros que você definiu estão de acordo com o esperado.

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` O arquivo está correto.

Após a reinicialização, você deve fazer login e visualizar o `running-config` arquivo e, em seguida, procure a descrição da interface 3/64, que é o rótulo da versão do 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. Ative as portas ISL no cs1, o switch 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 Link State deve indicar Up .

### 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. Ative a porta de cluster e2a em ambos os nós:

```
network port modify
```

### Mostrar exemplo

O exemplo a seguir mostra a porta e2a sendo ativada no nó 1 e no nó 2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

## Etapa 3: Validar 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
```

| Node  | Port | Role    | Link | MTU  | Auto-Negot<br>Admin/Oper | Duplex<br>Admin/Oper | Speed (Mbps)<br>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 o clus2 associado à porta e2a:

```
network interface revert
```

A 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 agora está em casa.(true ) em ambos os nós:

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

### Mostrar exemplo

```
cluster::*> network interface show -role cluster
```

| Vserver | Logical<br>Interface | Status<br>Admin/Oper | Network<br>Address/Mask | Current<br>Node | Current<br>Port | Is<br>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. Veja 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 salve o arquivo quando estiver satisfeito com as versões do software e as configurações do 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 switch, cs1.

**O que vem a seguir?**

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

**Instale o software FASTPATH e os RCFs para ONTAP 8.3.1 e versões posteriores.**

Siga este procedimento para instalar o software FASTPATH e os RCFs para ONTAP 8.3.1 e versões posteriores.

Os passos de instalação são os mesmos tanto para os switches de gerenciamento NetApp CN1601 quanto para os switches de cluster CN1610 que executam o ONTAP 8.3.1 ou posterior. No entanto, os dois modelos requerem software e RCFs diferentes.

## Requisitos de revisão

### Antes de começar

Certifique-se de ter o seguinte:

- Um backup atual da configuração do switch.
- Um cluster totalmente funcional (sem erros nos logs e sem placas de interface de rede (NICs) defeituosas ou problemas semelhantes).
- Conexões de porta totalmente funcionais no switch de cluster.
- Todas as portas do cluster estão configuradas.
- Todas as interfaces lógicas do cluster (LIFs) devem estar configuradas (não devem ter sido migradas).
- Um caminho de comunicação bem-sucedido: O ONTAP (privilegio: avançado) `cluster ping-cluster -node node1` O comando deve indicar que `larger than PMTU communication` **Tem sucesso em todos os caminhos.**
- Uma versão compatível de FASTPATH, RCF e ONTAP.

Certifique-se de consultar a tabela de compatibilidade de switches no "[Switches NetApp CN1601 e CN1610](#)" Página com as versões suportadas de FASTPATH, RCF e ONTAP .

### Instale o software FASTPATH

O procedimento a seguir utiliza a sintaxe clusterizada do Data ONTAP 8.2. Como resultado, o Vserver do cluster, os nomes LIF e a saída da CLI são diferentes daqueles presentes no Data ONTAP 8.3.

Pode haver dependências entre a sintaxe de comandos nas versões RCF e FASTPATH.



Na versão 1.2 do RCF, o suporte para Telnet foi explicitamente desativado devido a preocupações de segurança. Para evitar problemas de conectividade durante a instalação do RCF 1.2, verifique se o Secure Shell (SSH) está ativado. O "[Guia do Administrador do Switch NetApp CN1610](#)" Possui mais informações sobre SSH.

### Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de interruptor e nó:

- Os nomes dos dois switches NetApp são cs1 e cs2.
- Os nomes das interfaces lógicas de cluster (LIF) são node1\_clus1 e node1\_clus2 para o nó 1, e node2\_clus1 e node2\_clus2 para o nó 2. (É possível ter até 24 nós em um cluster.)
- O nome da máquina virtual de armazenamento (SVM) é Cluster.
- O `cluster1::*>` O prompt indica o nome do cluster.
- As portas do cluster em cada nó são denominadas e0a e e0b.

O "[Hardware Universe](#)" contém mais informações sobre as portas de cluster reais que são suportadas em sua plataforma.

- Os links entre switches (ISLs) suportados são as portas 0/13 a 0/16.
- As conexões de nó 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. Exibir informações sobre as LIFs no cluster:

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

### Mostrar exemplo

O exemplo a seguir mostra as interfaces lógicas no cluster. Neste exemplo, `-role` O parâmetro `cluster` exibe informações sobre as LIFs associadas às portas do 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
e0a node1_clus1 up/up 10.254.66.82/16 node1
true
e0b node1_clus2 up/up 10.254.206.128/16 node1
true
e0a node2_clus1 up/up 10.254.48.152/16 node2
true
e0b node2_clus2 up/up 10.254.42.74/16 node2
true
4 entries were displayed.
```

3. Em cada nó respectivo, usando uma LIF de gerenciamento de nós, migre `node1_clus2` para `e0a` no nó 1 e `node2_clus2` para `e0a` no nó 2:

```
network interface migrate
```

Você deve inserir os comandos nos consoles do controlador que possuem as respectivas LIFs do 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 este 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 LIF de cluster geral.

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, digitando "y" quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (\*>) é exibida.

6. Desative 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 as respectivas LIFs do cluster.

### Mostrar exemplo

O exemplo a seguir mostra os comandos para desativar 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 desativada 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. Desative as portas Inter-Switch Link (ISL) em 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 backup 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

## Etapa 2: Instale o software FASTPATH e o 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. Faça o download do arquivo de imagem para o switch.

Copiar o arquivo de imagem para a imagem ativa significa que, ao reiniciar, essa imagem estabelece a versão do FASTPATH em execução. A imagem anterior permanece disponível como backup.

**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 da imagem de inicialização atual e da próxima versão ativa:

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 com a nova versão da imagem no switch.

Se a versão do RCF já estiver correta, ative 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.
```



O `.scr` A extensão deve ser definida como parte do nome do arquivo antes de executar 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 é exibida no console.

5. Verifique se o script foi baixado e salvo com o nome de arquivo que você definiu.

### 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 interruptor.

### 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 interruptor 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!
```

## Etapa 3: Validar 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 reinicialização, você deve fazer login para verificar a versão da imagem, visualizar a configuração em execução e procurar a descrição na interface 3/64, que é o rótulo da versão do RCF.

2. Ative as portas ISL no cs1, o switch 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 Link State deve indicar Up .



### 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. Ative a porta de cluster e0b em todos os nós:

```
network port modify
```

Você deve inserir os comandos nos consoles do controlador que possuem as respectivas LIFs do cluster.

### Mostrar exemplo

O exemplo a seguir mostra a porta e0b sendo ativada no nó 1 e no nó 2:

```
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 agora está em casa.(true ) 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    |             |            |                    |         |
| e0a        | node1_clus1 | up/up      | 169.254.66.82/16   | node1   |
| e0b        | node1_clus2 | up/up      | 169.254.206.128/16 | node1   |
| e0a        | node2_clus1 | up/up      | 169.254.48.152/16  | node2   |
| e0b        | node2_clus2 | up/up      | 169.254.42.74/16   | node2   |

4 entries were displayed.

### 7. Exibir 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. Retornar ao nível de privilégio de administrador:

```
set -privilege admin
```

### 9. Repita os passos 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 seu ambiente de cluster,

consulte o ["Guia de Instalação e Configuração dos Switches CN1601 e CN1610"](#) .

## Migrar switches

**Migre de um ambiente de cluster sem switch para um ambiente de cluster NetApp CN1610 com switch.**

Se você já possui um ambiente de cluster sem switches com dois nós, pode migrar para um ambiente de cluster com switches com dois nós usando switches de rede de cluster CN1610, o que permite escalar para além de dois nós.

### Requisitos de revisão

#### Antes de começar

Certifique-se de ter o seguinte:

Para uma configuração sem switch de dois nós, certifique-se de que:

- A configuração sem switch de dois nós está configurada corretamente e funcionando.
- Os nós estão executando o ONTAP 8.2 ou posterior.
- Todas as portas do cluster estão no up estado.
- Todas as interfaces lógicas do cluster (LIFs) estão no up estado e em seus portos de origem.

Para a configuração do switch de cluster CN1610:

- A infraestrutura de comutadores de cluster CN1610 está totalmente funcional em ambos os switches.
- Ambos os switches possuem conectividade de rede de gerenciamento.
- É possível acessar os switches do cluster através do console.
- As conexões CN1610 entre nós e entre switches utilizam cabos twinax ou de fibra óptica.

O ["Hardware Universe"](#) Contém mais informações sobre cabeamento.

- Os cabos Inter-Switch Link (ISL) estão conectados às portas 13 a 16 em ambos os switches CN1610.
- A personalização inicial de ambos os switches CN1610 foi 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 dos switches CN1601 e CN1610"](#)
- ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#)

### Migre os switches

#### Sobre os exemplos

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- 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::*>` O prompt indica o nome do cluster.
- As portas de cluster utilizadas neste procedimento são e1a e e2a.

O "[Hardware Universe](#)" Contém as informações mais recentes sobre as portas de cluster reais para suas plataformas.

## Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

A mensagem avançada (`*>`) é exibida.

2. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

### Mostrar exemplo

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

```
cluster::*> system node autosupport invoke -node * -type all
-mmessage MAINT=2h
```

## Etapa 2: Configurar portas

1. Desative todas as portas voltadas para os nós (exceto as portas ISL) nos dois novos switches do cluster, cs1 e cs2.

Você não deve desativar as portas ISL.

### Mostrar exemplo

O exemplo a seguir mostra que as portas voltadas para o nó, de 1 a 12, 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 voltadas para o nó, de 1 a 12, 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 de cluster CN1610, cs1 e cs2, estão configurados corretamente. up :

```
show port-channel
```

## Mostrar exemplo

O exemplo a seguir mostra que as portas ISL são up no switch 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<br>Ports | Device/<br>Timeout         | Port<br>Speed | Port<br>Active |
|--------------|----------------------------|---------------|----------------|
| -----        | -----                      | -----         | -----          |
| 0/13         | actor/long<br>partner/long | 10G Full      | True           |
| 0/14         | actor/long<br>partner/long | 10G Full      | True           |
| 0/15         | actor/long<br>partner/long | 10G Full      | True           |
| 0/16         | actor/long<br>partner/long | 10G Full      | True           |

O exemplo a seguir mostra que as portas ISL são up no switch 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 conectados 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 do cluster está conectada à porta correspondente no nó do cluster parceiro:

```
run * cdpd show-neighbors
```

#### Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster e1a e e2a estão conectadas à mesma porta no nó parceiro do cluster:

```
cluster::*> run * cdpd show-neighbors
2 entries were acted on.
```

Node: node1

| Local Remote | Remote    | Remote   | Remote | Hold |
|--------------|-----------|----------|--------|------|
| Port Device  | Interface | Platform | Time   |      |
| Capability   |           |          |        |      |

|     |       |     |         |     |
|-----|-------|-----|---------|-----|
| e1a | node2 | e1a | FAS3270 | 137 |
| H   |       |     |         |     |
| e2a | node2 | e2a | FAS3270 | 137 |
| H   |       |     |         |     |

Node: node2

| Local Remote | Remote    | Remote   | Remote | Hold |
|--------------|-----------|----------|--------|------|
| Port Device  | Interface | Platform | Time   |      |
| Capability   |           |          |        |      |

|     |       |     |         |     |
|-----|-------|-----|---------|-----|
| e1a | node1 | e1a | FAS3270 | 161 |
| H   |       |     |         |     |
| e2a | node1 | e2a | FAS3270 | 161 |
| H   |       |     |         |     |

6. Verifique se todos os LIFs do cluster estão up e operacional:

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

Cada LIF de cluster deve exibir `true` na coluna “É o Lar”.

## Mostrar exemplo

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

|            | Logical   | Status     | Network       | Current |      |
|------------|-----------|------------|---------------|---------|------|
| Current Is |           |            |               |         |      |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node    | Port |
| Home       |           |            |               |         |      |
| -----      | -----     | -----      | -----         | -----   |      |
| node1      |           |            |               |         |      |
| true       | clus1     | up/up      | 10.10.10.1/16 | node1   | e1a  |
| true       | clus2     | up/up      | 10.10.10.2/16 | node1   | e2a  |
| node2      |           |            |               |         |      |
| true       | clus1     | up/up      | 10.10.11.1/16 | node2   | e1a  |
| true       | clus2     | up/up      | 10.10.11.2/16 | node2   | e2a  |

4 entries were displayed.



Os comandos de modificação e migração descritos nas etapas 10 a 13 devem ser executados a partir do nó local.

7. Verifique se todas as portas do cluster estão 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 para `false` nos LIFs de cluster `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 posteriores, utilize o seguinte comando: `network interface modify -vserver Cluster -lif * -auto-revert false`

9. Verifique a conectividade das interfaces do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. **[[passo 10]]** 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 de clus1 para a porta e2a nos nós 1 e 2:

```

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 posteriores, utilize 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 no nó 1 e no nó 2:

```
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. Desative a porta e1a do cluster em ambos os nós:

```
network port modify
```

### Mostrar exemplo

O exemplo a seguir mostra como desativar a porta e1a no nó 1 e no nó 2:

```
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 estado da porta:

```
network port show
```

## Mostrar exemplo

O exemplo a seguir mostra que a porta e1a é down nos nós 1 e 2:

```
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.

- Desconecte o cabo da porta do cluster e1a no nó 1 e, em seguida, conecte e1a à porta 1 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches CN1610.

O "[Hardware Universe](#)" Contém mais informações sobre cabeamento.

- Desconecte o cabo da porta do cluster e1a no nó 2 e, em seguida, conecte e1a à porta 2 no switch do cluster cs1, usando o cabeamento apropriado suportado pelos switches CN1610.
- Habilite todas as portas voltadas para o nó no switch de cluster cs1.

## Mostrar exemplo

O exemplo a seguir mostra que as portas de 1 a 12 estão habilitadas 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
```

- Ative a primeira porta do cluster, e1a, em cada nó:

```
network port modify
```

### Mostrar exemplo

O exemplo a seguir mostra como habilitar a porta e1a no nó 1 e no nó 2:

```
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 estão up :

```
network port show -ipSPACE Cluster
```

### Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão up nos nós 1 e 2:

```
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 o clus1 para a porta e1a no nó 1 e no nó 2:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```



Para a versão 8.3 e posteriores, utilize o seguinte comando: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

11. Verifique se todos os LIFs do cluster estão up , operacional e exibido como true na coluna "É o Lar":

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

### Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs são up nos nós 1 e 2 e que os resultados da coluna "É 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 estado 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 o 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 no nó 1 e no nó 2:

```
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 posteriores, utilize 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 no nó 1 e no nó 2:

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

|            | Logical   | Status     | Network       | Current |       |
|------------|-----------|------------|---------------|---------|-------|
| Current Is |           |            |               |         |       |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node    | Port  |
| Home       |           |            |               |         |       |
| -----      | -----     | -----      | -----         | -----   | ----- |
| node1      |           |            |               |         |       |
| true       | clus1     | up/up      | 10.10.10.1/16 | node1   | e1a   |
| false      | clus2     | up/up      | 10.10.10.2/16 | node1   | e1a   |
| node2      |           |            |               |         |       |
| true       | clus1     | up/up      | 10.10.11.1/16 | node2   | e1a   |
| false      | clus2     | up/up      | 10.10.11.2/16 | node2   | e1a   |

4 entries were displayed.

15. Desative a porta e2a do cluster em ambos os nós:

```
network port modify
```

### Mostrar exemplo

O exemplo a seguir mostra como desativar a porta e2a nos nós 1 e 2:

```
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 estado da porta:

```
network port show
```

### Mostrar exemplo

O exemplo a seguir mostra que a porta e2a é down nos nós 1 e 2:

```
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. Desconecte o cabo da porta do cluster e2a no nó 1 e, em seguida, conecte e2a à porta 1 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches CN1610.
18. Desconecte o cabo da porta do cluster e2a no nó 2 e, em seguida, conecte e2a à porta 2 no switch do cluster cs2, usando o cabeamento apropriado suportado pelos switches CN1610.
19. Habilite todas as portas voltadas para os nós no switch de cluster cs2.

### Mostrar exemplo

O exemplo a seguir mostra que as portas de 1 a 12 estão habilitadas 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. Habilite a segunda porta do cluster, e2a, em cada nó.

### Mostrar exemplo

O exemplo a seguir mostra como habilitar a porta e2a no nó 1 e no nó 2:

```
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 estão up :

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

### Mostrar exemplo

O exemplo a seguir mostra que todas as portas do cluster estão up nos nós 1 e 2:

```
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 o clus2 para a porta e2a no nó 1 e no nó 2:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```



Para a versão 8.3 e posteriores, os comandos são:

```
cluster::*> network interface revert -vserver Cluster -lif
node1_clus2 e
cluster::*> network interface revert -vserver Cluster -lif
node2_clus2
```

## Etapa 3: Conclua a configuração

1. Verifique se todas as interfaces estão sendo exibidas. true na coluna "É o Lar":

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

## Mostrar exemplo

O exemplo a seguir mostra que todos os LIFs são up nos nós 1 e 2 e que os resultados da coluna "É Casa" são true :

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

| Current Is | Logical   | Status     | Network       | Current |
|------------|-----------|------------|---------------|---------|
| 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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. [[passo 3]] Verifique se ambos os nós têm duas conexões com cada switch:

```
show isdp neighbors
```

## Mostrar exemplo

O exemplo a seguir mostra os resultados apropriados para ambas as opções:

```
(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. Exibir informações sobre os dispositivos na sua configuração:

```
network device discovery show
```

3. Desative as configurações de configuração 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 interruptor:

```
cluster::*> network options detect-switchless modify -enabled false
```



Para a versão 9.2 e posteriores, ignore esta etapa, pois a configuração é convertida automaticamente.

4. Verifique se as configurações estão desativadas:

```
network options detect-switchless-cluster show
```

**Mostrar exemplo**

O false O resultado 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 posteriores, aguarde até `Enable Switchless Cluster` está definido como falso. Isso pode levar até três minutos.

5. Configure os clusters `clus1` e `clus2` para reverter automaticamente 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 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 posteriores, utilize 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 nós membros do cluster:

```
cluster show
```

### Mostrar exemplo

O exemplo a seguir mostra informações sobre a saúde 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 desativou a criação automática de casos, reative-a enviando uma mensagem do 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 administrador:

```
set -privilege admin
```

## Substitua os interruptores

### Substitua um switch de cluster NetApp CN1610

Siga estes passos para substituir um switch NetApp CN1610 defeituoso em uma rede cluster. Este é um procedimento não disruptivo (NDU).

#### Requisitos de revisão

##### Antes de começar

Antes de efetuar a substituição do switch, as seguintes condições devem ser atendidas no ambiente atual e no switch de substituição, considerando a infraestrutura de cluster e rede existente:

- O cluster existente deve ser verificado como totalmente funcional, com pelo menos um switch de cluster totalmente conectado.
- Todas as portas do cluster devem estar **ativas**.
- Todas as interfaces lógicas do cluster (LIFs) devem estar ativas e não devem ter sido migradas.
- O cluster ONTAP `ping-cluster -node node1` O comando deve indicar que a conectividade básica e a comunicação com dispositivos maiores que PMTU estão funcionando corretamente em todos os caminhos.

#### Ativar registro no console

A NetApp recomenda enfaticamente que você habilite o registro de console nos dispositivos que estiver usando e execute as seguintes ações ao substituir seu switch:

- Mantenha o AutoSupport ativado durante a manutenção.
- Execute uma manutenção AutoSupport antes e depois da manutenção para desativar a criação de chamados durante o período de manutenção. Consulte este artigo da Knowledge Base ["SU92: Como suprimir a criação automática de chamados durante janelas de manutenção programadas"](#) para obter mais detalhes.
- Ative o registro de sessões para todas as sessões da CLI. Para obter instruções sobre como ativar o registro de sessão, consulte a seção "Registro de saída da sessão" neste artigo da Base de Conhecimento. ["Como configurar o PuTTY para obter conectividade ideal com sistemas ONTAP"](#).

#### Substitua o interruptor

##### Sobre esta tarefa

Você deve executar o comando para migrar um LIF de cluster a partir do nó onde o LIF de cluster está hospedado.

Os exemplos neste procedimento utilizam a seguinte nomenclatura de comutador de cluster e nó:

- Os nomes dos dois switches de cluster CN1610 são `cs1` e `cs2`.
- O nome do interruptor CN1610 que deve ser substituído (o interruptor defeituoso) é `old_cs1`.
- O nome do novo switch CN1610 (o switch 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 o 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 o 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 arquivo deve ter a extensão `.scr`.

1. [[passo 3]]Salve o arquivo de configuração em execução do switch em um host externo, preparando-o 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 do switch e do ONTAP correspondem na matriz de compatibilidade. Consulte ["Switches NetApp CN1601 e CN1610"](#) para obter detalhes.
3. Na ["Página de Downloads de Software"](#) NetApp Support Site, selecione NetApp Cluster Switches para baixar as versões apropriadas do RCF e do FASTPATH.
4. Configure um servidor TFTP (Trivial File Transfer Protocol) com FASTPATH, RCF e configuração salva. `.scr` Arquivo para uso com o novo switch.
5. Conecte a porta serial (o conector RJ-45 identificado como "IOIOI" no lado direito do switch) a um host disponível com emulação de terminal.
6. No computador host, configure as opções de conexão do terminal serial:
  - a. 9600 baud

- b. 8 bits de dados
  - c. 1 bit de parada
  - d. paridade: nenhuma
  - e. Controle de fluxo: nenhum
7. Conecte a porta de gerenciamento (a porta RJ-45 com conector em forma de chave inglesa no lado esquerdo do switch) à mesma rede onde o seu servidor TFTP está localizado.
8. Prepare-se para conectar-se à rede com o servidor TFTP.

Se você estiver usando o Protocolo de Configuração Dinâmica de Hosts (DHCP), não precisa configurar um endereço IP para o switch neste momento. A porta de serviço está configurada para usar DHCP por padrão. A porta de gerenciamento de rede está definida como "nenhuma" nas configurações de protocolo IPv4 e IPv6. Se a porta do seu dispositivo estiver conectada a uma rede que possui um servidor DHCP, as configurações do servidor serão configuradas automaticamente.

Para definir um endereço IP estático, você deve usar os comandos `serviceport protocol`, `network protocol` e `serviceport ip`.

#### Mostrar exemplo

```
(new_cs1) # serviceport ip <ipaddr> <netmask> <gateway>
```

9. Opcionalmente, se o servidor TFTP estiver em um laptop, conecte o switch CN1610 ao laptop usando um cabo Ethernet padrão e, em seguida, configure sua porta de rede na mesma rede com um endereço IP alternativo.

Você pode usar o `ping` comando para verificar o endereço. Caso não consiga estabelecer a conectividade, utilize uma rede não roteada e configure a porta de serviço usando o endereço IP 192.168.x ou 172.16.x. Você poderá reconfigurar a porta de serviço para o endereço IP de gerenciamento de produção posteriormente.

10. Opcionalmente, verifique e instale as versões apropriadas dos softwares RCF e FASTPATH para o novo switch. Se você verificou que o novo switch está configurado corretamente e não requer atualizações do software RCF e FASTPATH, você deve ir para a etapa 13.
- a. Verifique as novas configurações do interruptor.

#### Mostrar exemplo

```
(new_cs1) > enable
(new_cs1) # show version
```

- b. Faça o download do RCF para o novo switch.

### 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 arquivo RCF foi baixado para o switch.

### 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 ao interruptor 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. Faça o download da imagem para o switch 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 precisa ser reinicializado para que o comando na etapa 6 reflita a nova imagem. Existem duas possíveis visualizações para a resposta que você poderá ver após inserir o comando de recarregamento.

### 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 previamente salva ao novo switch.

**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, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

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

x representa a duração da janela de manutenção em horas.



A mensagem do AutoSupport notifica o suporte técnico sobre essa tarefa de manutenção, de forma que a criação automática de chamados seja suprimida durante o período de manutenção.

13. No novo switch new\_cs1, faça login como usuário administrador e desligue todas as portas conectadas às interfaces do cluster de nós (portas de 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 do cluster das portas que estão conectadas ao switch old\_cs1.

Você deve migrar cada LIF do 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 do cluster foram movidas para a porta de cluster apropriada em cada nó.

### Mostrar exemplo

```
cluster::> network interface show -role cluster
```

16. Desligue as portas do cluster que estão conectadas 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 desativadas.

#### Mostrar exemplo

```
cluster::*> cluster ping-cluster -node <node_name>
```

19. No switch CS2, desative as portas ISL de 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 preparado para a substituição do switch.
21. Remova todos os cabos do switch antigo (old\_cs1) e, em seguida, conecte os cabos às mesmas portas no switch novo (new\_cs1).
22. No switch CS2, ative as portas ISL de 13 a 16.

#### Mostrar exemplo

```
(cs2)# config
(cs2)(config)# interface 0/13-0/16
(cs2)(interface 0/13-0/16)# no shutdown
```

23. Ative as portas no novo switch que estão associadas aos nós do 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, ative a porta do nó do cluster que está conectada ao switch substituído e, em seguida, confirme se o link está ativo.

**Mostrar exemplo**

```
cluster::*> network port modify -node nodel -port
<port_to_be_online> -up-admin true
cluster::*> network port show -role cluster
```

25. Reverta as LIFs do cluster associadas à porta na etapa 25 no mesmo nó.

Neste exemplo, as LIFs no nó 1 são revertidas com sucesso se a coluna “É Residência” for verdadeira.

**Mostrar exemplo**

```
cluster::*> network interface revert -vserver nodel -lif
<cluster_lif_to_be_reverted>
cluster::*> network interface show -role cluster
```

26. Se a LIF do cluster do primeiro nó estiver ativa e revertida para sua porta inicial, repita os passos 25 e 26 para ativar as portas do cluster e reverter as LIFs do cluster nos outros nós do cluster.
27. Exibir informações sobre os nós do 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 da etapa 1.

**Mostrar exemplo**

```
(new_cs1)> enable
(new_cs1)# show running-config
(new_cs1)# show startup-config
```

29. Se você desativou a criação automática de casos, reative-a enviando uma mensagem do 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 uma em que dois nós estão conectados diretamente no ONTAP 9.3 e versões posteriores.

### Requisitos de revisão

#### Diretrizes

Analise as seguintes diretrizes:

- A migração para uma configuração de cluster sem switches com dois nós é uma operação não disruptiva. A maioria dos sistemas possui duas portas de interconexão de cluster dedicadas em cada nó, mas você também pode usar este 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 já possui um cluster de dois nós que utiliza switches de interconexão de cluster e está executando o ONTAP 9.3 ou posterior, pode substituir os switches por conexões diretas, ponto a ponto, entre os nós.

#### Antes de começar

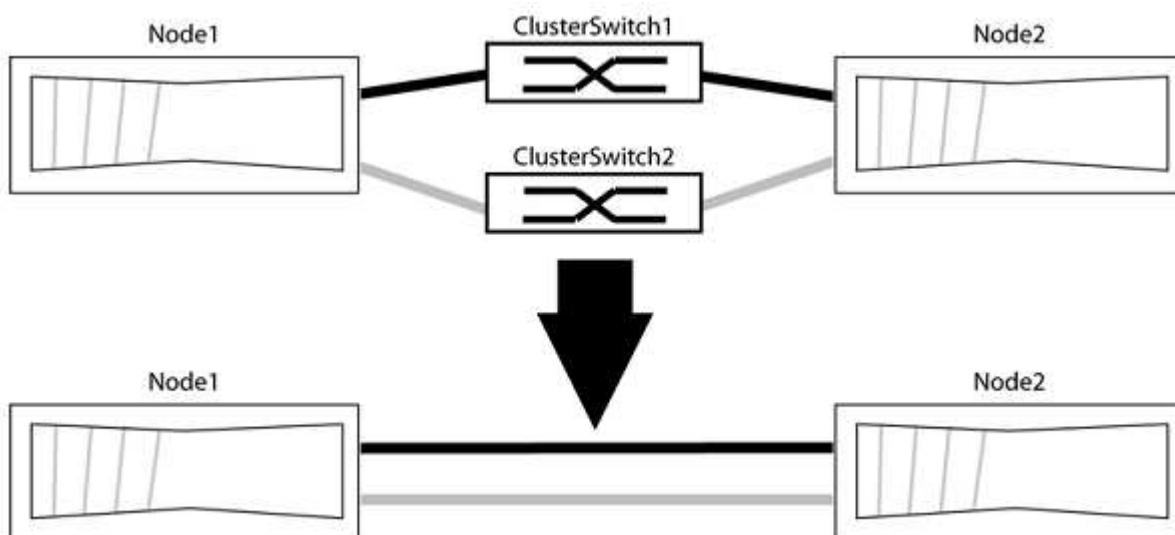
Certifique-se de ter o seguinte:

- Um cluster saudável consiste em dois nós conectados por switches de cluster. Os nós devem estar executando a mesma versão do ONTAP .
- Cada nó possui o número necessário de portas de cluster dedicadas, que fornecem conexões de interconexão de cluster redundantes para suportar a configuração do seu sistema. Por exemplo, existem duas portas redundantes para um sistema com duas portas de interconexão de cluster dedicadas em cada nó.

#### Migre 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 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 elas variam de acordo com o sistema.

### Etapa 1: Prepare-se para a migração

1. Altere o nível de privilégio para avançado, inserindo `y` Quando solicitado a continuar:

```
set -privilege advanced
```

O prompt avançado `*>` aparece.

2. O ONTAP 9.3 e versões posteriores suportam a detecção automática de clusters sem switch, recurso que está habilitado por padrão.

Você pode verificar se a detecção de clusters sem switch está habilitada executando o comando de privilégios avançados:

```
network options detect-switchless-cluster show
```

#### Mostrar exemplo

O exemplo de saída a seguir mostra se a opção está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Ativar detecção de cluster sem switch" estiver ativado `false` Entre em contato com o suporte da NetApp .

3. Se o AutoSupport estiver ativado neste cluster, suprima a criação automática de casos invocando uma mensagem do AutoSupport :

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

onde `h` é a duração da janela de manutenção em horas. A mensagem notifica o suporte técnico sobre essa tarefa de manutenção para que eles possam impedir a criação automática de chamados durante o período de manutenção.

No exemplo a seguir, o comando suprime a criação automática de casos por duas horas:

#### Mostrar exemplo

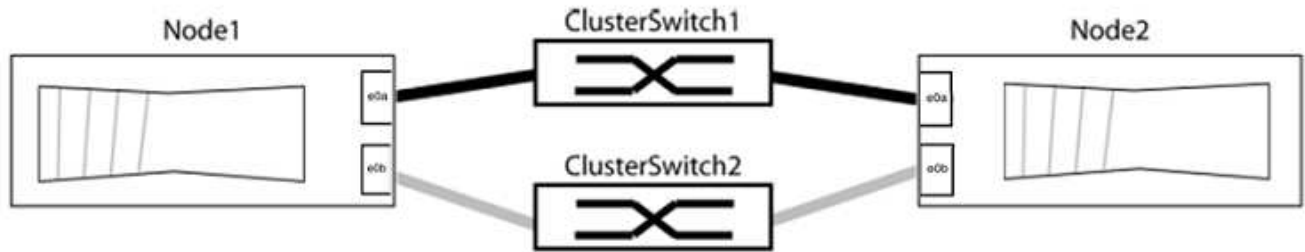
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

## Etapa 2: Configurar portas e cabos

1. Organize as portas de cluster em cada switch em grupos, de forma que as portas de cluster do grupo 1 sejam conectadas ao switch de cluster 1 e as portas de cluster do grupo 2 sejam conectadas ao switch de cluster 2. Esses grupos serão necessários mais tarde no procedimento.
2. Identifique as portas do cluster e verifique o status e a integridade dos links:

```
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, pois elas variam de sistema para sistema.



Verifique se as portas têm um valor de `up` para a coluna "Link" e um valor de `healthy` para a coluna "Estado de Saúde".

### 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 do cluster estão em suas portas de origem.

Verifique se a coluna “is-home” está `true` para cada um dos LIFs do 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 estejam em suas portas de origem, reverta essas LIFs para suas portas de origem:

```
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 conectadas a um switch de rede:

```
network device-discovery show -port cluster_port
```

A coluna “Dispositivo Descoberto” deve conter o nome do switch do cluster ao qual a porta está conectada.

## Mostrar exemplo

O exemplo a seguir mostra que as portas de cluster "e0a" e "e0b" estão corretamente conectadas aos switches de 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet |                          | Source      | Destination |
|--------|--------------------------|-------------|-------------|
| 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   |                          |             |             |

## Todas as versões do ONTAP

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

```
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. [[passo 7]] Verifique se o cluster está íntegro:

```
cluster ring show
```

Todas as unidades devem ser mestras ou secundárias.

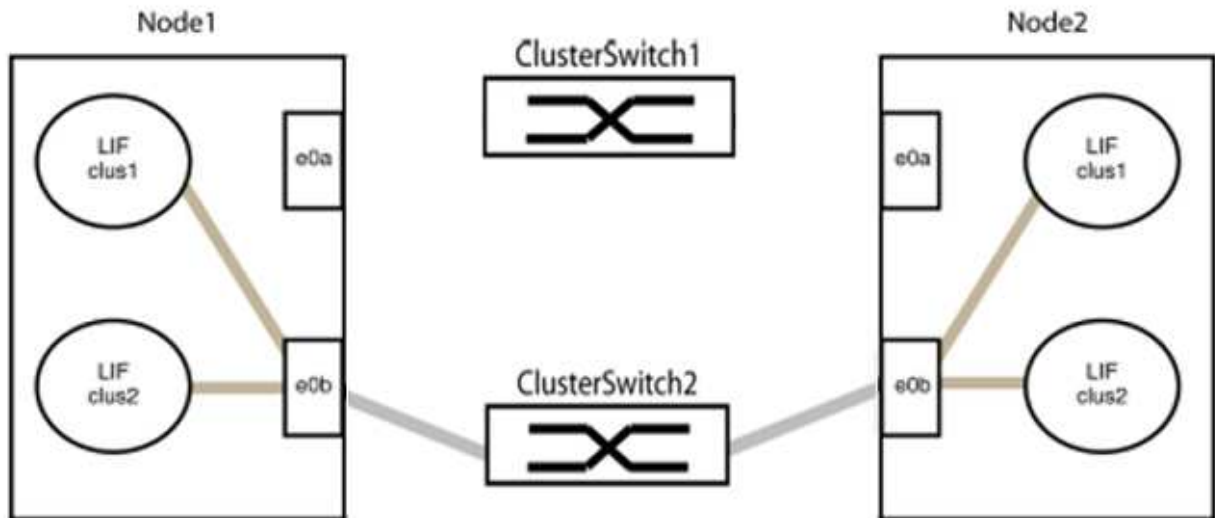
2. Configure a configuração sem switch para as portas do grupo 1.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 1 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

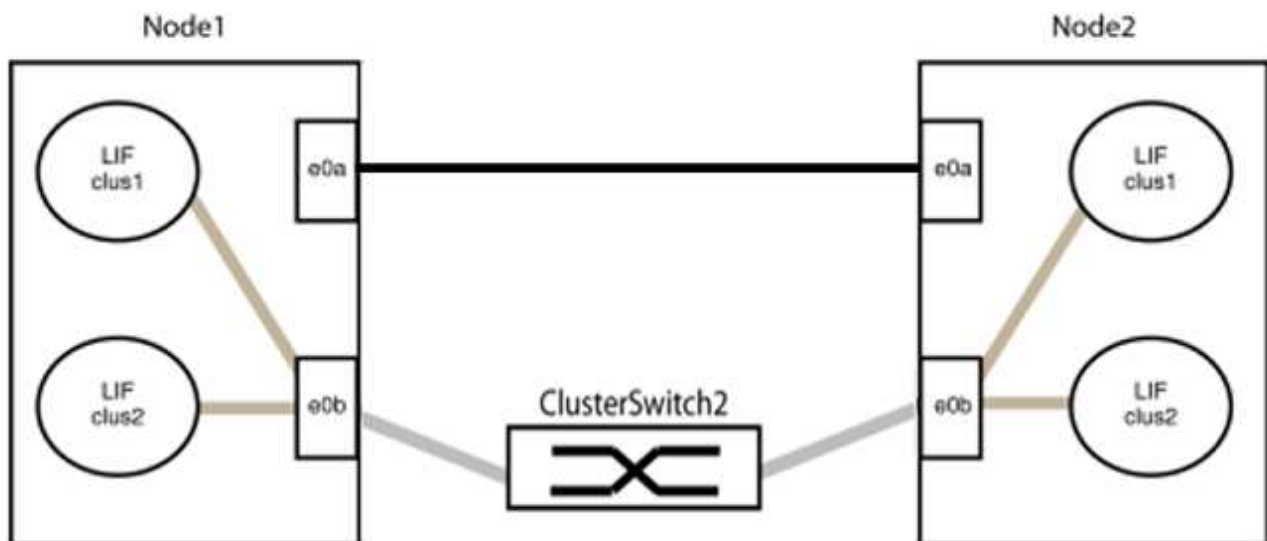
- a. Desconecte todos os cabos das portas do grupo 1 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0a" em cada nó, e o tráfego do cluster continua através do switch e da porta "e0b" em cada nó:



b. Conecte os cabos das portas do grupo 1 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2:



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 interruptor 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 do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet                   | Source      | Destination |
|--------------------------|-------------|-------------|
| Node                     | LIF         | LIF         |
| Date                     |             |             |
| 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 |
| 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                     |             |             |

## Todas as versões do ONTAP

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

```
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 aguardar pelo menos dois minutos para confirmar uma conexão back-to-back funcional no grupo 1.

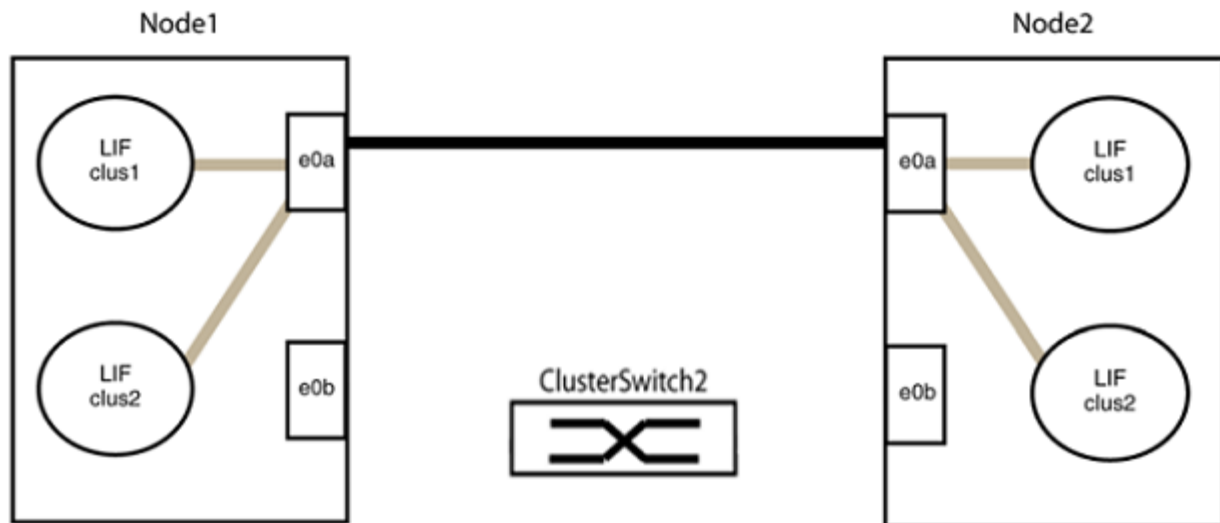
1. Configure a configuração sem switch para as portas no grupo 2.



Para evitar possíveis problemas de rede, você deve desconectar as portas do grupo 2 e reconectá-las consecutivamente o mais rápido possível, por exemplo, **em menos de 20 segundos**.

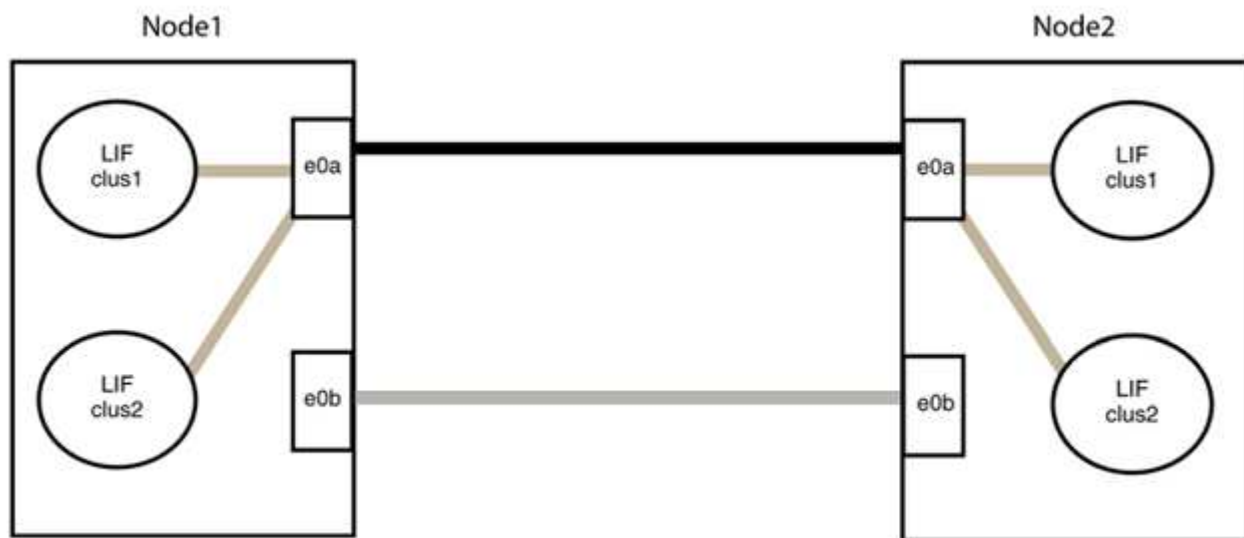
- a. Desconecte todos os cabos das portas do grupo 2 simultaneamente.

No exemplo a seguir, os cabos são desconectados da porta "e0b" em cada nó, e o tráfego do cluster continua através da conexão direta entre as portas "e0a":



b. Conecte os cabos das portas do grupo 2 em sequência.

No exemplo a seguir, "e0a" no nó 1 está conectado a "e0a" no nó 2 e "e0b" no nó 1 está conectado a "e0b" no nó 2:



### Etapa 3: Verifique a configuração

1. Verifique se as portas em ambos os nós estão corretamente conectadas:

```
network device-discovery show -port cluster_port
```

## Mostrar exemplo

O exemplo a seguir mostra que as portas do cluster "e0a" e "e0b" estão corretamente conectadas à porta correspondente no parceiro do 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 valores de LIF foram revertidos se a coluna "Is Home" estiver marcada. `true` , conforme 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 algum LIFS do cluster não tiver retornado às suas portas originais, reverta-os manualmente a partir do nó local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Verifique o status do cluster dos nós no console do sistema de qualquer um dos nós:

```
cluster show
```

### Mostrar exemplo

O exemplo a seguir mostra o valor de epsilon em ambos os nós. `false` :

```
Node Health Eligibility Epsilon

node1 true true false
node2 true true false
2 entries were displayed.
```

5. Verifique a conectividade das interfaces do cluster remoto:

## ONTAP 9.9.1 e posterior

Você pode usar o `network interface check cluster-connectivity` Comando para iniciar uma verificação de acessibilidade para conectividade do 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:** Aguarde alguns segundos antes de executar o `show` comando para exibir os detalhes.

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

| Packet |                          | Source      | Destination |
|--------|--------------------------|-------------|-------------|
| 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   |                          |             |             |

## Todas as versões do ONTAP

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

```
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. **[[passo 6]]** Se você desativou a criação automática de casos, reative-a invocando uma mensagem do AutoSupport :

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

Para mais informações, consulte ["Artigo 1010449 da Base de Conhecimento da NetApp : Como suprimir a criação automática de casos durante janelas de manutenção programadas"](#).

2. Altere o nível de privilégio de volta para administrador:

```
set -privilege admin
```

# Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

## Direitos autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](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/"](https://www.netapp.com/company/legal/privacy-policy/)

## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; 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 DESTES DOCUMENTOS, 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.