



Configurar software

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-systems-switches/switch-cisco-3132q-v/configure-software-overview-3132q-v-cluster.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Índice

- Configurar software 1
 - Fluxo de trabalho de instalação de software para switches de cluster Cisco Nexus 3132Q-V 1
 - Configure o switch Cisco Nexus 3132Q-V. 1
 - Prepare-se para instalar o software NX-OS e o arquivo de configuração de referência. 4
 - Instale o software NX-OS. 11
 - Requisitos de revisão 11
 - Instale o software 11
 - Instale ou atualize o RCF 28
 - Visão geral da instalação ou atualização do Arquivo de Configuração de Referência (RCF) 29
 - Instale o arquivo de configuração de referência (RCF) 31
 - Atualize seu Arquivo de Configuração de Referência (RCF) 41
 - Verifique sua configuração SSH. 62
 - Redefinir o switch do cluster 3132Q-V para os padrões de fábrica 64

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.

6

"Restaure as configurações de fábrica do switch."

Apague as configurações do switch do cluster 3132Q-V.

Configure o switch Cisco Nexus 3132Q-V.

Siga este procedimento para configurar o switch Cisco Nexus 3132Q-V.

Antes de começar

- Acesso a um servidor HTTP, FTP ou TFTP no 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 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 concluídas. Ver "[Folha de trabalho completa de cabeamento do Cisco Nexus 3132Q-V](#)".
- Arquivos RCF aplicáveis para rede de cluster e rede de gerenciamento da NetApp, baixados do site de suporte da NetApp em "meusuporte.netapp.com" para os interruptores que você receber. 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 possuem a versão atual do software NX-OS, mas não têm os arquivos RCF 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 _Instalação de um switch de cluster Cisco Nexus 3132Q-V e painel de passagem em um gabinete NetApp 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 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.
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 os bits-chave de 1024 a 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 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 .

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 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 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)

```

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
```

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-
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 obter mais informações sobre os comandos da Cisco , consulte o guia apropriado em ["Guias de referência 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
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-
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 C3132Q-V	cluster-network	10.233.205.90	N3K-
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 Base de Conhecimento ["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. Selecione a versão RCF aplicável à

sua configuração. Ver ["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**. Veja 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.

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 -ipspace Cluster
```

Mostrar exemplo

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

```
Node: cluster1-01
```

```
Ignore
```

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

e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
8 entries were displayed.
```

```
Node: cluster1-03
```

```
Ignore
```

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

e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

```
Node: cluster1-04
```

```
Ignore
```

Speed (Mbps)

```

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

```

b. Verifique se todas as interfaces de cluster (LIFs) estão na porta 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
-is-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.

- 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::*>				

- 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 o artigo da Base de Conhecimento. ["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 -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

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 o bootflash do switch cs2 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 "[Guia de Comandos do Cisco Nexus Série 3000 NX-OS](#)" guias.

Mostrar exemplo

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

14. 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"](#) guias.

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 etapas sobre como colocar suas portas 10GbE on-line após uma atualização do RCF, consulte o artigo da Base de conhecimento ["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 em ["Guia de Comandos do Cisco Nexus Série 3000 NX-OS"](#) guias.

Mostrar exemplo

```
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

17. 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
```

18. Reaplique quaisquer personalizações anteriores à configuração do switch. Consulte "[Analise as considerações sobre cabeamento e configuração](#)." Para obter detalhes sobre quaisquer alterações adicionais necessárias.

19. 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					
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.

20. 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.

21. 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::*>				

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 1 a 19 no switch cs1.

24. Ative a reversão automática nos LIFs do cluster.

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

25. 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 Loss	LIF	LIF
-----	-----	
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`. 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"](#).

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.

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 SOBRESSALENTE; 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 SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

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

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

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

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

Informações sobre marcas comerciais

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