



Configurar o software

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-systems-switches/switch-cisco-9336c-fx2-storage/configure-software-overview-9336c-storage.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Índice

Configurar o software	1
Fluxo de trabalho de instalação de software para switches de armazenamento Cisco Nexus 9336C-FX2 e 9336C-FX2-T	1
Configurar os switches de armazenamento 9336C-FX2 e 9336C-FX2-T	1
Prepare-se para instalar ou atualizar o software NX-OS e o RCF	4
Instale ou atualize o software NX-OS	10
Requisitos de revisão	10
Instale o software	11
Instale ou atualize o RCF	33
Visão geral da instalação ou atualização do Arquivo de Configuração de Referência (RCF)	33
Instale o arquivo de configuração de referência	35
Atualize seu Arquivo de Configuração de Referência (RCF)	46
Verifique sua configuração SSH	55
Redefinir os switches de armazenamento 9336C-FX2 e 9336C-FX2-T para os padrões de fábrica	57

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.

6

"Restaure as configurações de fábrica do switch."

Apague as configurações dos switches de armazenamento 9336C-FX2 e 9336C-FX2-T.

Configurar os switches de armazenamento 9336C-FX2 e 9336C-FX2-T

Siga este procedimento para configurar os switches Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Antes de começar

Certifique-se de 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 para o interruptor. Ver ["Documentação necessária"](#) para mais informações.


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.	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.

Incitar	Resposta
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)	<p>Responda com sim. A opção padrão é sim.</p> <div>  <p>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.</p> </div>
Digite o tipo de chave SSH que deseja gerar (dsa/rsa/ras1).	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)	<p>Responda com sim para salvar a configuração. Isso atualiza automaticamente as imagens do Kickstart e do sistema.</p> <div>  <p>Se você não salvar a configuração nesta etapa, nenhuma das alterações terá efeito na próxima vez que você reiniciar o switch.</p> </div>

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 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 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 lldp
```

Mostrar exemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/lldp				
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/lldp				
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

4. Verifique o status administrativo ou operacional de cada interface 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
```

```
Ignore
```

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
4 entries were displayed.
```

b. Exibir informações sobre os LIFs:

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


Mostrar exemplo

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

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	3/5/2024	19:21:18	-06:00	cluster1-01_clus2	cluster1-02
clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-01_clus2	cluster1-
02_clus2	none				
node2					
	3/5/2024	19:21:18	-06:00	cluster1-02_clus2	cluster1-
01_clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-02_clus2	cluster1-
01 clus2	none				

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

8

```

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 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 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"](#)

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, 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 -ipospace 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 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 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 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 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. Ver "[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.

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 e 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. Selecione a versão RCF aplicável à sua configuração. Ver "[Switches Ethernet da Cisco](#)" para mais informações.

Nome da RCF
Cluster-HA-Breakout RCF 1.xx

Nome da RCF
Cluster-HA-Storage RCF 1.xx
Armazenamento RCF 1.xx
MultiCluster-HA RCF 1.xx

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 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.

Veja 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 Base de Conhecimento. ["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 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 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 Cisco , consulte o guia apropriado no ["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-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 9000 NX-OS"](#) .

Mostrar exemplo

Este exemplo mostra o RCF Nexus_9336C_RCF_v1.6-Storage.txt sendo instalado no switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-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

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Storage.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*****
*****
```

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

```
show running-config
```

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.

```
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 Base de Conhecimento "[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. 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
```

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

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

13. Reinicie o interruptor cs1.

```
cs1# reload

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

14. Repita os passos 1 a 13 no switch cs2.
15. Conecte as portas 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
mgmt0  --          up      <mgmt ip address>
1000    1500
Eth1/11      1      eth  trunk  up      none
100G(D)  --
Eth1/12      1      eth  trunk  up      none
100G(D)  --
Eth1/13      1      eth  trunk  up      none
100G(D)  --
Eth1/14      1      eth  trunk  up      none
100G(D)  --
Eth1/15      1      eth  trunk  up      none
100G(D)  --
Eth1/16      1      eth  trunk  up      none
100G(D)  --
Eth1/17      1      eth  trunk  up      none
100G(D)  --
Eth1/18      1      eth  trunk  up      none
100G(D)  --
Eth1/23      1      eth  trunk  up      none
100G(D)  --
Eth1/24      1      eth  trunk  up      none
100G(D)  --
Eth1/25      1      eth  trunk  up      none
100G(D)  --
Eth1/26      1      eth  trunk  up      none
100G(D)  --
Eth1/27      1      eth  trunk  up      none
100G(D)  --
Eth1/28      1      eth  trunk  up      none
100G(D)  --
Eth1/29      1      eth  trunk  up      none
100G(D)  --
Eth1/30      1      eth  trunk  up      none
100G(D)  --
```

2. Verifique se os nós 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	Po999
30	VLAN0030	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/16, Eth1/17 Eth1/18, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth1/25, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/35 Eth1/36

```
cs1# show interface trunk
```

Port	Native 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.

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 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.



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 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
-----
node1-01/cdp
           e3a     cs1                Ethernet1/7    N9K-
C9336C
           e3b     cs2                Ethernet1/7    N9K-
C9336C
node1-02/cdp
           e3a     cs1                Ethernet1/8    N9K-
C9336C
           e3b     cs2                Ethernet1/8    N9K-
C9336C
.
.
.
```

4. 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						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

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> enable
cs1# configure
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(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.

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
```

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

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

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, utilize uma ferramenta de comparação ou de diferenças 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 Base de Conhecimento "[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. 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 Cisco , consulte o guia apropriado no "[Guia de Comandos do Cisco Nexus Série 9000 NX-OS](#)" guias.

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-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)...
```

13. 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 9000 NX-OS](#)" guias.

Este exemplo mostra o arquivo RCF. `NX9336C-FX2-RCF-v1.13-1-Storage.txt` sendo instalado no switch `cs1`:

```
cs1# copy Nexus_9336C_RCF_v1.6-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.

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.
16. 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 Cisco , consulte o guia apropriado no "[Guia de Comandos do Cisco Nexus Série 9000 NX-OS](#)" guias.

```
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 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	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

19. 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.
```

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

21. 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
```

2. Verifique se os nós esperados ainda estão conectados:

```
show cdp neighbors
```

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

```
show vlan brief
```

```
show interface trunk
```

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

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

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>
```

5. Verifique se o cluster está íntegro:

```
cluster show
```

6. 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
```

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

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


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`. Ver ["Configure a segurança de rede usando FIPS."](#) Para obter 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
```

```
(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.

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 SOBRESSALIENTES; 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.