



Configurar el software

Cluster and storage switches

NetApp
April 25, 2024

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems-switches/switch-cisco-3132q-v/prepare-install-cisco-nexus-3132q.html> on April 25, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Configurar el software 1
 - Prepare la instalación del software NX-OS y del archivo de configuración de referencia 1
 - Instale el software NX-OS 6
 - Instalación del archivo de configuración de referencia (RCF) 13
 - Recopilación de registro de supervisión del estado del switch Ethernet 38
 - Configurar SNMPv3 41

Configurar el software

Prepare la instalación del software NX-OS y del archivo de configuración de referencia

Antes de instalar el software NX-OS y el archivo de configuración de referencia (RCF), siga este procedimiento.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan dos nodos. Estos nodos utilizan dos puertos de interconexión de clúster de 10 GbE e0a y.. e0b.

Consulte "[Hardware Universe](#)" para verificar los puertos de clúster correctos en sus plataformas.



Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `cluster1-01` y.. `cluster1-02`.
- Los nombres de LIF del clúster son `cluster1-01_clus1` y.. `cluster1-01_clus2` para `cluster1-01` y.. `cluster1-02_clus1` y.. `cluster1-02_clus2` para `cluster1-02`.
- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Pasos

1. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

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

donde `x` es la duración de la ventana de mantenimiento en horas.



El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

2. Cambie el nivel de privilegio a avanzado, introduciendo `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

3. Muestre cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

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

Muestra el ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e0a	cs1	Eth1/2	N3K-
C3132Q-V	e0b	cs2	Eth1/2	N3K-
C3132Q-V				
cluster1-01/cdp	e0a	cs1	Eth1/1	N3K-
C3132Q-V	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

4. Compruebe el estado administrativo u operativo de cada interfaz de clúster.

a. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

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

Node: cluster1-02

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

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

Node: cluster1-01

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

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

b. Mostrar información acerca de las LIF:

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

Muestra el ejemplo

```
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. Haga ping en las LIF de clúster remoto:

```
cluster ping-cluster -node local
```

Muestra el ejemplo

```
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)
```

6. Compruebe que el auto-revert El comando está habilitado en todos los LIF de clúster:

```
network interface show -vserver Cluster -fields auto-revert
```

Muestra el ejemplo

```
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

El futuro

["Instale el software NX-OS".](#)

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3132Q-V.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).

Documentación sugerida

- ["Switch Ethernet de Cisco"](#). Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de actualización y software adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el software

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Asegúrese de completar el procedimiento en ["Prepare la instalación del software NX-OS y del archivo de configuración de referencia"](#)y, a continuación, siga los pasos que se indican a continuación.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja el software NX-OS y el RCF.

Muestra el ejemplo

```
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. Copie el software NX-OS en el switch Nexus 3132Q-V utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía adecuada en ["Guías de referencia de comandos Cisco Nexus serie 3000 NX-OS"](#).

Muestra el ejemplo

```
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.
```

4. Compruebe la versión que se está ejecutando del software NX-OS:

```
show version
```

Muestra el ejemplo

```
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#
```

5. Instale la imagen NX-OS.

La instalación del archivo de imagen hace que se cargue cada vez que se reinicia el conmutador.

Muestra el ejemplo

```
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#
```

6. Compruebe la nueva versión del software NX-OS una vez que se haya reiniciado el switch:

```
show version
```

Muestra el ejemplo

```
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#
```

El futuro

["Instalación del archivo de configuración de referencia \(RCF\)".](#)

Instalación del archivo de configuración de referencia (RCF)

Siga este procedimiento para instalar el RCF después de configurar por primera vez el interruptor Nexus 3132Q-V. También puede utilizar este procedimiento para actualizar la versión de RCF.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El archivo de configuración de referencia actual (RCF).
- Una conexión de consola al conmutador, necesaria para instalar el RCF.
- ["Switch Ethernet de Cisco"](#). Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la que se encuentra en las versiones de NX-OS.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de actualización y software adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el archivo

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y `cs2`.
- Los nombres de nodo son `cluster1-01`, `cluster1-02`, `cluster1-03`, y `cluster1-04`.
- Los nombres de LIF del clúster son `cluster1-01_clus1`, `cluster1-01_clus2`, `cluster1-02_clus1`, `cluster1-02_clus2`, `cluster1-03_clus1`, `cluster1-03_clus2`, `cluster1-04_clus1`, y `cluster1-04_clus2`.

```
04_clus1,y.cluster1-04_clus2.
```

- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Durante este procedimiento no se necesita ningún enlace entre switches (ISL) operativo. Esto se debe a que los cambios en la versión de RCF pueden afectar temporalmente a la conectividad ISL. Para garantizar operaciones de clúster no disruptivas, el siguiente procedimiento migra todas las LIF del clúster al switch de partner operativo mientras realiza los pasos del switch de destino.

Asegúrese de completar el procedimiento en "[Prepare la instalación del software NX-OS y del archivo de configuración de referencia](#)", y, a continuación, siga los pasos que se indican a continuación.

Paso 1: Compruebe el estado del puerto

1. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```


Muestra el ejemplo

```
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. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster tengan el estado correcto:

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

Muestra el ejemplo

```
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. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

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

Muestra el ejemplo

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

Current	Logical	Status	Network	
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. Compruebe que el clúster muestra información de ambos switches de clúster:

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

Muestra el ejemplo

```
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 y versiones posteriores, utilice el comando `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Deshabilite la reversión automática en las LIF del clúster.

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

Asegúrese de que la reversión automática esté deshabilitada después de ejecutar este comando.

4. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos.

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

5. Comprobar que los puertos del clúster han migrado a los puertos alojados en el switch cs1 del clúster. Esto puede tardar unos segundos.

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

Muestra el ejemplo

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a false			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0a false			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0a false			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0a false			

```
cluster1::*>
```

6. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
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::*>
```

Paso 2: Configurar y verificar la configuración

1. Si aún no lo ha hecho, guarde una copia de la configuración actual del conmutador copiando la salida del siguiente comando en un archivo de texto:

```
show running-config
```

2. Limpie la configuración del interruptor cs2 y realice una configuración básica.



Al actualizar o aplicar una nueva RCF, debe borrar los ajustes del conmutador y realizar la configuración básica. Debe estar conectado al puerto de la consola de serie del switch para volver a configurar el switch.

- a. Limpie la configuración:

Muestra el ejemplo

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

- b. Reinicie el conmutador:

Muestra el ejemplo

```
(cs2)# reload

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

3. Copie el RCF en el bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

```
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)...
```

4. Aplique el RCF descargado anteriormente al flash de inicio.

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

5. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir las instrucciones que se indican en **Notas importantes** para garantizar la configuración y el funcionamiento correctos del interruptor.

Muestra el ejemplo

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3132Q-V
* Filename  : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : Nov-02-2020
* Version   : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports 7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```

* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*   - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*     NX-OS using a version later than 9.3(5).
*   - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*   - After the RCF is applied and switch rebooted, then proceed to
upgrade
*     NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*   after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*   hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*   hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*   hardware profile front portmode qsfp      (To reset to QSFP)
*
*****
*****

```

6. Compruebe que el archivo RCF es la versión más reciente correcta:

```
show running-config
```

Cuando compruebe la salida para verificar que tiene el RCF correcto, asegúrese de que la siguiente información es correcta:

- El banner de RCF
- La configuración del nodo y el puerto
- Personalizaciones

La salida varía en función de la configuración del sitio. Compruebe la configuración del puerto y consulte las notas de versión para conocer los cambios específicos del RCF que haya instalado.



Para conocer los pasos sobre cómo conectar sus puertos 10GbE después de una actualización de RCF, consulte el artículo de la base de conocimientos ["Los puertos 10GbE de un switch de clúster Cisco 3132Q no se conectan"](#).

7. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo running-config en el archivo startup-config.

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

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

8. Reinicie el interruptor cs2. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

Muestra el ejemplo

```
cs2# reload
This command will reboot the system. (y/n)? [n] y
```

9. Aplique el mismo RCF y guarde la configuración en ejecución por segunda vez.

Muestra el ejemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
cs2# copy running-config startup-config
[#####] 100% Copy complete
```

10. Compruebe el estado de los puertos del clúster en el clúster.
 - a. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

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

Muestra el ejemplo

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Compruebe el estado del switch del clúster.

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

Muestra el ejemplo

```
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 y versiones posteriores, utilice el comando `system switch ethernet show -is-monitoring-enabled-operational true`.

Puede observar la siguiente salida en la consola del conmutador cs1 dependiendo de la versión RCF cargada previamente en el conmutador:



```
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.
```

+



Los nodos del clúster pueden tardar hasta 5 minutos en informar en buen estado.

11. En el switch de clúster cs1, apague los puertos conectados a los puertos del clúster de los nodos.

Muestra el ejemplo

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
```

12. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch cs2. Esto puede tardar unos segundos.

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

Muestra el ejemplo

```
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::*>
```

13. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
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 los pasos del 1 al 10 en el interruptor cs1.
15. Habilite la reversión automática en las LIF del clúster.

Muestra el ejemplo

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

16. Reinicie el interruptor cs1. Para activar las LIF de clúster y revertir a sus puertos raíz, haga lo siguiente. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

```
cs1# reload  
This command will reboot the system. (y/n)? [n] y
```

Paso 3: Verificar la configuración

1. Compruebe que los puertos del switch conectados a los puertos del clúster estén activos.

```
show interface brief | grep up
```

Muestra el ejemplo

```
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. Compruebe que el ISL entre cs1 y cs2 funciona:

```
show port-channel summary
```

Muestra el ejemplo

```
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. Compruebe que las LIF del clúster han vuelto a su puerto de inicio:

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

Muestra el ejemplo

```
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. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
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. Haga ping en las interfaces de clúster remoto para verificar la conectividad:

```
cluster ping-cluster -node local
```

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

6. Para ONTAP 9.8 y versiones posteriores, habilite la función de recogida de registros de control de estado

del switch de Ethernet para recopilar archivos de registro relacionados con el switch mediante los comandos:

```
system switch ethernet log setup-password y..
```

```
system switch ethernet log enable-collection
```

a. Introduzca: `system switch ethernet log setup-password`

Muestra el ejemplo

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

b. Introduzca: `system switch ethernet log enable-collection`

Muestra el ejemplo

```
cluster1::*> system switch ethernet log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

7. Para las versiones 9.5P16, 9.6P12 y 9.7P10 de ONTAP y versiones posteriores de parches, habilite la función de recopilación de registros del monitor de estado del switch Ethernet para recopilar archivos de registro relacionados con el switch mediante los comandos:

```
system cluster-switch log setup-password y..
```

```
system cluster-switch log enable-collection
```

- a. Introduzca: `system cluster-switch log setup-password`

Muestra el ejemplo

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

b. Introduzca: `system cluster-switch log enable-collection`

Muestra el ejemplo

```
cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Recopilación de registro de supervisión del estado del switch Ethernet

Es posible usar la función de recopilación de registros para recoger archivos de registro relacionados con switches en ONTAP.

El monitor de estado del switch Ethernet (CSHM) es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración. Este procedimiento lo guía a través del proceso de configuración e inicio de la recopilación de registros detallados de **Soporte** desde el switch e inicia una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

Antes de empezar

- Compruebe que ha configurado su entorno mediante el conmutador de clúster de Cisco 3132Q-V **CLI**.
- La monitorización del estado del interruptor debe estar activada para el interruptor. Verifique esto asegurándose de que el `Is Monitored:` el campo se establece en **true** en la salida del `system switch ethernet show` comando.

Pasos

1. Cree una contraseña para la función de recogida de registros de monitor de estado del switch Ethernet:

```
system switch ethernet log setup-password
```


Muestra el ejemplo

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Para iniciar la recopilación de registros, ejecute el siguiente comando, sustituyendo EL DISPOSITIVO por el conmutador utilizado en el comando anterior. Esto inicia ambos tipos de recopilación de registros: Los registros detallados de **Support** y una recopilación horaria de datos **Periódicos**.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Muestra el ejemplo

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Espere 10 minutos y compruebe que se complete la recogida de registros:

```
system switch ethernet log show
```



Si alguno de estos comandos devuelve un error o si la recogida de registros no se completa, póngase en contacto con el soporte de NetApp.

Resolución de problemas

Si se encuentra con alguno de los siguientes estados de error informados por la función de recopilación de registros (visible en la salida de `system switch ethernet log show`), pruebe los pasos de depuración correspondientes:

Estado de error de recopilación de registros	Resolución
Las claves RSA no están presentes	Vuelva a generar las claves SSH de ONTAP. Póngase en contacto con el soporte de NetApp.
error de contraseña de cambio	Verifique las credenciales, pruebe la conectividad SSH y vuelva a generar las claves SSH de ONTAP. Revise la documentación del switch o póngase en contacto con el soporte de NetApp para obtener instrucciones.
Las claves ECDSA no están presentes para FIPS	Si el modo FIPS está activado, es necesario generar claves ECDSA en el conmutador antes de volver a intentarlo.

registro preexistente encontrado	Elimine el archivo de recopilación de registros anterior del conmutador.
error de registro de volcado del interruptor	Asegúrese de que el usuario del conmutador tiene permisos de recopilación de registros. Consulte los requisitos previos anteriores.

Configurar SNMPv3

Siga este procedimiento para configurar SNMPv3, que admite la monitorización del estado del switch Ethernet (CSHM).

Acerca de esta tarea

Los siguientes comandos configuran un nombre de usuario SNMPv3 en switches Cisco 3132Q-V.

- Para **sin autenticación**: `snmp-server user SNMPv3_USER NoAuth`
- Para **autenticación MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Para autenticación **MD5/SHA con cifrado AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Pasos

1. Configure el usuario SNMPv3 en el conmutador para que utilice autenticación y cifrado:

```
show snmp user
```

Muestra el ejemplo

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                                SNMP USERS
-----
-----

User          Auth          Priv(enforce)  Groups
acl_filter
-----
-----
admin          md5          des(no)        network-admin
SNMPv3User     md5          aes-128(no)    network-operator
-----
-----

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User          Auth          Priv
-----
-----

(sw1) (Config)#
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Muestra el ejemplo

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure CSHM para monitorizar con el nuevo usuario de SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```

Muestra el ejemplo

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado el período de sondeo de CSHM.

```
system switch ethernet polling-interval show
```

Muestra el ejemplo

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.