



# **Configurare il software**

## **Cluster and storage switches**

NetApp  
April 25, 2024

# Sommario

- Configurare il software ..... 1
  - Preparare l'installazione del software NX-OS e del file di configurazione di riferimento ..... 1
  - Installare il software NX-OS ..... 6
  - Installazione del file di configurazione di riferimento (RCF)..... 13
  - Raccolta registro monitoraggio stato switch Ethernet ..... 38
  - Configurare SNMPv3 ..... 41

# Configurare il software

## Preparare l'installazione del software NX-OS e del file di configurazione di riferimento

Prima di installare il software NX-OS e il file di configurazione di riferimento (RCF), seguire questa procedura.

### A proposito degli esempi

Gli esempi di questa procedura utilizzano due nodi. Questi nodi utilizzano due porte di interconnessione cluster da 10 GbE e0a e e0b.

Vedere ["Hardware Universe"](#) per verificare le porte cluster corrette sulle piattaforme.



Gli output dei comandi possono variare a seconda delle diverse versioni di ONTAP.

Gli esempi di questa procedura utilizzano la seguente nomenclatura di switch e nodi:

- I nomi dei due switch Cisco sono `cs1` e `cs2`.
- I nomi dei nodi sono `cluster1-01` e `cluster1-02`.
- I nomi LIF del cluster sono `cluster1-01_clus1` e `cluster1-01_clus2` per i `cluster1-01` e `cluster1-02_clus1` e `cluster1-02_clus2` per il `cluster1-02`.
- Il `cluster1: *>` prompt indica il nome del cluster.

### A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 3000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

### Fasi

1. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

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

dove `x` è la durata della finestra di manutenzione in ore.



Il messaggio AutoSupport informa il supporto tecnico di questa attività di manutenzione in modo che la creazione automatica del caso venga soppressa durante la finestra di manutenzione.

2. Impostare il livello di privilegio su Advanced (avanzato), immettendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (`*>`).

3. Visualizza quante interfacce di interconnessione cluster sono configurate in ciascun nodo per ogni switch

di interconnessione cluster:

network device-discovery show -protocol cdp

**Mostra esempio**

```
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. Controllare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.

a. Visualizzare gli attributi della porta di rete:

network port show -ipspace Cluster

## Mostra esempio

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

Node: cluster1-02

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

Node: cluster1-01

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

b. Visualizzare le informazioni sui LIF:

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

Mostra esempio

```
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. Ping delle LIF del cluster remoto:

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

## Mostra esempio

```
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. Verificare che il auto-revert Il comando è attivato su tutte le LIF del cluster:

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

## Mostra esempio

```
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

Quali sono le prossime novità?

["Installare il software NX-OS"](#).

## Installare il software NX-OS

Seguire questa procedura per installare il software NX-OS sullo switch del cluster Nexus 3132Q-V.

### Verifica dei requisiti

#### Di cosa hai bisogno

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).

#### Documentazione consigliata

- ["Switch Ethernet Cisco"](#). Consultare la tabella di compatibilità degli switch per le versioni supportate di ONTAP e NX-OS.
- ["Switch Cisco Nexus serie 3000"](#). Consultare le guide all'aggiornamento e al software appropriate disponibili sul sito Web di Cisco per la documentazione completa sulle procedure di aggiornamento e downgrade dello switch Cisco.

## Installare il software

### A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 3000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

Assicurarsi di completare la procedura descritta in ["Preparare l'installazione del software NX-OS e del file di configurazione di riferimento"](#), quindi seguire la procedura riportata di seguito.

### Fasi



1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare `ping` Comando per verificare la connettività al server che ospita il software NX-OS e RCF.

#### Mostra esempio

```
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. Copiare il software NX-OS sullo switch Nexus 3132Q-V utilizzando uno dei seguenti protocolli di trasferimento: FTP, TFTP, SFTP o SCP. Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Guide di riferimento per Cisco Nexus 3000 Series NX-OS Command"](#).

#### Mostra esempio

```
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. Verificare la versione in esecuzione del software NX-OS:

```
show version
```

## Mostra esempio

```
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. Installare l'immagine NX-OS.

L'installazione del file immagine ne provoca il caricamento ogni volta che lo switch viene riavviato.

## Mostra esempio

```
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. Verificare la nuova versione del software NX-OS dopo il riavvio dello switch:

```
show version
```

## Mostra esempio

```
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#
```

### Quali sono le prossime novità?

["Installazione del file di configurazione di riferimento \(RCF\)".](#)

## Installazione del file di configurazione di riferimento (RCF)

Seguire questa procedura per installare RCF dopo aver configurato lo switch Nexus 3132Q-V per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

### Verifica dei requisiti

#### Di cosa hai bisogno

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Il file di configurazione di riferimento corrente (RCF).
- Una connessione console allo switch, necessaria per l'installazione di RCF.
- ["Switch Ethernet Cisco"](#). Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Si noti che esistono dipendenze di comando tra la sintassi del comando in RCF e quella presente nelle versioni di NX-OS.
- ["Switch Cisco Nexus serie 3000"](#). Consultare le guide all'aggiornamento e al software appropriate disponibili sul sito Web di Cisco per la documentazione completa sulle procedure di aggiornamento e downgrade dello switch Cisco.

### Installare il file

#### A proposito degli esempi

Gli esempi di questa procedura utilizzano la seguente nomenclatura di switch e nodi:

- I nomi dei due switch Cisco sono `cs1` e `cs2`.
- I nomi dei nodi sono `cluster1-01`, `cluster1-02`, `cluster1-03`, e `cluster1-04`.
- I nomi LIF del cluster sono `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.
```

- Il `cluster1::*>` prompt indica il nome del cluster.

### A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 3000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

Durante questa procedura non è necessario alcun collegamento interswitch operativo (ISL). Ciò è dovuto alla progettazione, in quanto le modifiche alla versione di RCF possono influire temporaneamente sulla connettività ISL. Per garantire operazioni del cluster senza interruzioni, la seguente procedura esegue la migrazione di tutte le LIF del cluster allo switch del partner operativo durante l'esecuzione delle operazioni sullo switch di destinazione.

Assicurarsi di completare la procedura descritta in ["Preparare l'installazione del software NX-OS e del file di configurazione di riferimento"](#), quindi seguire la procedura riportata di seguito.

### Fase 1: Controllare lo stato della porta

1. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster:

```
network device-discovery show
```



## Mostra esempio

```
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. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.

a. Verificare che tutte le porte del cluster siano funzionanti:

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

## Mostra esempio

```
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. Verificare che tutte le interfacce del cluster (LIF) siano sulla porta home:

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

## Mostra esempio

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
Home				
-----				
-----				
Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			
cluster1::*>				

c. Verificare che il cluster visualizzi le informazioni per entrambi gli switch del cluster:

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

## Mostra esempio

```
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.
```



Per ONTAP 9.8 e versioni successive, utilizzare il comando `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Disattiva l'autorevert sulle LIF del cluster.

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

Assicurarsi che l'autorevert sia disattivato dopo aver eseguito questo comando.

4. Sullo switch del cluster cs2, spegnere le porte collegate alle porte del cluster dei nodi.

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

5. Verificare che le porte del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi.

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

#### Mostra esempio

```
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. Verificare che il cluster funzioni correttamente:

```
cluster show
```

### Mostra esempio

```
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::*>
```

## Fase 2: Configurare e verificare l'installazione

1. Se non è già stato fatto, salvare una copia della configurazione corrente dello switch copiando l'output del seguente comando in un file di testo:

```
show running-config
```

2. Pulire la configurazione sullo switch cs2 ed eseguire una configurazione di base.



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Per configurare nuovamente lo switch, è necessario essere collegati alla porta della console seriale dello switch.

- a. Pulire la configurazione:

### Mostra esempio

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Riavviare lo switch:

### Mostra esempio

```
(cs2)# reload

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

3. Copiare l'RCF nella flash di avvio dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: FTP, TFTP, SFTP o SCP. Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Cisco Nexus 3000 Series NX-OS Command Reference"](#) guide.

#### Mostra esempio

```
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. Applicare l'RCF precedentemente scaricato al bootflash.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Cisco Nexus 3000 Series NX-OS Command Reference"](#) guide.

#### Mostra esempio

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

5. Esaminare l'output dello striscione da `show banner motd` comando. Leggere e seguire le istruzioni in **Note importanti** per garantire la corretta configurazione e il corretto funzionamento dello switch.



## Mostra esempio

```
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. Verificare che il file RCF sia la versione più recente corretta:

```
show running-config
```

Quando si controlla l'output per verificare che l'RCF sia corretto, assicurarsi che le seguenti informazioni siano corrette:

- Il banner RCF
- Le impostazioni di nodo e porta
- Personalizzazioni

L'output varia in base alla configurazione del sito. Controllare le impostazioni della porta e fare riferimento alle note di rilascio per eventuali modifiche specifiche all'RCF installato.



Per informazioni su come portare le porte 10GbE in linea dopo un aggiornamento dell'RCF, consultare l'articolo della Knowledge base ["Le porte 10GbE su uno switch cluster Cisco 3132Q non sono disponibili in linea"](#).

#### 7. Dopo aver verificato che le versioni RCF e le impostazioni dello switch siano corrette, copiare il file running-config nel file startup-config.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Cisco Nexus 3000 Series NX-OS Command Reference"](#) guide.

#### Mostra esempio

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

8. Riavviare lo switch cs2. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

#### Mostra esempio

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

9. Applicare lo stesso RCF e salvare la configurazione in esecuzione per una seconda volta.

#### Mostra esempio

```
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. Verificare lo stato delle porte del cluster sul cluster.

- a. Verificare che le porte del cluster siano funzionanti in tutti i nodi del cluster:

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

## Mostra esempio

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

b. Verificare lo stato dello switch dal cluster.

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

## Mostra esempio

```
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.

```



Per ONTAP 9.8 e versioni successive, utilizzare il comando `system switch ethernet show -is-monitoring-enabled-operational true`.

A seconda della versione RCF precedentemente caricata sullo switch, sulla console dello switch cs1 potrebbero essere presenti i seguenti output:



```

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.

```

+



I nodi del cluster possono richiedere fino a 5 minuti per il reporting come integri.

11. Sullo switch del cluster cs1, spegnere le porte collegate alle porte del cluster dei nodi.

#### Mostra esempio

```

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

```

12. Verificare che le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi.

```

network interface show -vserver Cluster

```

### Mostra esempio

```
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. Verificare che il cluster funzioni correttamente:

```
cluster show
```

### Mostra esempio

```
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. Ripetere i passaggi da 1 a 10 sullo switch cs1.
15. Abilitare il ripristino automatico sulle LIF del cluster.

#### Mostra esempio

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

16. Riavviare lo switch cs1. Questa operazione consente di attivare le LIF del cluster per ripristinare le porte home. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

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

### Fase 3: Verificare la configurazione

1. Verificare che le porte dello switch collegate alle porte del cluster siano in funzione.

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

#### Mostra esempio

```
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. Verificare che l'ISL tra cs1 e cs2 funzioni correttamente:

```
show port-channel summary
```

### Mostra esempio

```
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. Verificare che le LIF del cluster siano tornate alla porta home:

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

### Mostra esempio

```
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. Verificare che il cluster funzioni correttamente:

```
cluster show
```

### Mostra esempio

```
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. Eseguire il ping delle interfacce del cluster remoto per verificare la connettività:

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

**Mostra esempio**

```
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. Per ONTAP 9.8 e versioni successive, attivare la funzione di raccolta dei log dello switch Ethernet per la

raccolta dei file di log relativi allo switch utilizzando i comandi seguenti:

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

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

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

#### Mostra esempio

```
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. Inserire: `system switch ethernet log enable-collection`

### Mostra esempio

```
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::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

7. Per le release di patch ONTAP 9.5P16, 9.6P12 e 9.7P10 e successive, attivare la funzione di raccolta dei log di Health monitor dello switch Ethernet per la raccolta dei file di log relativi allo switch utilizzando i comandi:

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

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

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

### Mostra esempio

```
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. Inserire: `system cluster-switch log enable-collection`

### Mostra esempio

```
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::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

## Raccolta registro monitoraggio stato switch Ethernet

È possibile utilizzare la funzione di raccolta dei log per raccogliere i file di log relativi allo switch in ONTAP.

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug. Questa procedura guida l'utente attraverso il processo di impostazione e avvio della raccolta di registri **supporto** dettagliati dal centralino e avvia una raccolta oraria di dati **periodici** raccolti da AutoSupport.

### Prima di iniziare

- Verificare di aver configurato l'ambiente utilizzando lo switch cluster Cisco 3132Q-V **CLI**.
- Il monitoraggio dello stato dello switch deve essere abilitato per lo switch. Verificare questo assicurandosi che `Is Monitored:` il campo è impostato su **true** nell'output di `system switch ethernet show` comando.

### Fasi

1. Creare una password per la funzione di raccolta dei log dello switch Ethernet Health monitor:

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



## Mostra esempio

```
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. Per avviare la raccolta dei log, eseguire il comando seguente, sostituendo DEVICE con lo switch utilizzato nel comando precedente. Questo avvia entrambi i tipi di raccolta di log: I log dettagliati **Support** e una raccolta oraria di dati **Periodic**.

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

## Mostra esempio

```
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.
```

Attendere 10 minuti, quindi verificare che la raccolta del registro sia completata:

```
system switch ethernet log show
```



Se uno di questi comandi restituisce un errore o se la raccolta dei log non viene completata, contattare il supporto NetApp.

## Risoluzione dei problemi

Se si verifica uno dei seguenti stati di errore segnalati dalla funzione di raccolta registri (visibile nell'output di `system switch ethernet log show`), provare i passi di debug corrispondenti:

Stato errore raccolta log	Risoluzione
Chiavi RSA non presenti	Rigenerare le chiavi SSH ONTAP. Contattare l'assistenza NetApp.
errore password cambio	Verificare le credenziali, verificare la connettività SSH e rigenerare le chiavi SSH ONTAP. Per istruzioni, consultare la documentazione dello switch o contattare l'assistenza NetApp.
Chiavi ECDSA non presenti per FIPS	Se la modalità FIPS è attivata, le chiavi ECDSA devono essere generate sullo switch prima di riprovare.
trovato log preesistente	Rimuovere il file di raccolta del registro precedente sullo switch.

#### errore registro dump switch

Assicurarsi che l'utente dello switch disponga delle autorizzazioni per la raccolta dei registri. Fare riferimento ai prerequisiti riportati sopra.

## Configurare SNMPv3

Seguire questa procedura per configurare SNMPv3, che supporta il monitoraggio dello stato dello switch Ethernet (CSHM).

### A proposito di questa attività

I seguenti comandi configurano un nome utente SNMPv3 sugli switch Cisco 3132Q-V:

- Per **nessuna autenticazione**: `snmp-server user SNMPv3_USER NoAuth`
- Per l'autenticazione **MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Per l'autenticazione **MD5/SHA con crittografia AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

### Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
show snmp user
```

## Mostra esempio

```
(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. Impostare l'utente SNMPv3 sul lato ONTAP:

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

## Mostra esempio

```
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. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

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

## Mostra esempio

```
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. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

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

## Mostra esempio

```
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::*>
```

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.