



Configurare il software

Install and maintain

NetApp

February 13, 2026

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

Sommario

- Configurare il software 1
 - Flusso di lavoro di installazione del software per gli switch cluster Cisco Nexus 3132Q-V 1
 - Configurare lo switch Cisco Nexus 3132Q-V 1
 - Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento 4
 - Installa il software NX-OS 10
 - Requisiti di revisione 10
 - Installa il software 10
 - Installare o aggiornare l'RCF 27
 - Panoramica sull'installazione o l'aggiornamento del file di configurazione di riferimento (RCF) 28
 - Installare il file di configurazione di riferimento (RCF) 30
 - Aggiorna il tuo file di configurazione di riferimento (RCF) 40
 - Verifica la tua configurazione SSH 61
 - Ripristinare lo switch del cluster 3132Q-V ai valori predefiniti di fabbrica 63

Configurare il software

Flusso di lavoro di installazione del software per gli switch cluster Cisco Nexus 3132Q-V

Per installare e configurare il software per uno switch Cisco Nexus 3132Q-V e installare o aggiornare il file di configurazione di riferimento (RCF), attenersi alla seguente procedura:

1

"Configurare l'interruttore"

Configurare lo switch cluster 3132Q-V.

2

"Prepararsi all'installazione del software NX-OS e RCF"

Il software Cisco NX-OS e RCF devono essere installati sugli switch cluster Cisco 3132Q-V.

3

"Installa o aggiorna il software NX-OS"

Scaricare e installare o aggiornare il software NX-OS sullo switch cluster Cisco 3132Q-V.

4

"Installare o aggiornare l'RCF"

Installare o aggiornare l'RCF dopo aver configurato lo switch Cisco 3132Q-V.

5

"Verifica la configurazione SSH"

Verificare che SSH sia abilitato sugli switch per utilizzare le funzionalità di monitoraggio dello stato dello switch Ethernet (CSHM) e di raccolta dei registri.

6

"Ripristinare l'interruttore alle impostazioni predefinite di fabbrica"

Cancellare le impostazioni dello switch del cluster 3132Q-V.

Configurare lo switch Cisco Nexus 3132Q-V

Seguire questa procedura per configurare lo switch Cisco Nexus 3132Q-V.

Prima di iniziare

- Accesso a un server HTTP, FTP o TFTP nel sito di installazione per scaricare le versioni NX-OS e RCF (Reference Configuration File) applicabili.
- Versione NX-OS applicabile, scaricata da ["Scarica il software Cisco"](#) pagina.
- Documentazione richiesta per lo switch di rete, la documentazione del controller e la documentazione ONTAP . Per maggiori informazioni, vedere ["Documentazione richiesta"](#).
- Licenze applicabili, informazioni di rete e configurazione e cavi.

- Schede di lavoro sui cablaggi completate. Vedere ["Foglio di lavoro completo sul cablaggio Cisco Nexus 3132Q-V"](#) .
- RCF applicabili alla rete di cluster NetApp e alla rete di gestione, scaricabili dal sito di supporto NetApp all'indirizzo ["mysupport.netapp.com"](http://mysupport.netapp.com) per gli switch che ricevi. Tutti gli switch di rete cluster e di rete di gestione Cisco vengono forniti con la configurazione predefinita di fabbrica Cisco . Questi switch dispongono anche della versione corrente del software NX-OS, ma non hanno gli RCF caricati.

Passi

1. Installare gli switch e i controller della rete del cluster e della rete di gestione.

Se stai installando il tuo...	Poi...
Cisco Nexus 3132Q-V in un cabinet di sistema NetApp	Per istruzioni sull'installazione dello switch in un cabinet NetApp , consultare la guida _Installazione di uno switch cluster Cisco Nexus 3132Q-V e di un pannello pass-through in un cabinet NetApp .
Apparecchiature in un rack Telco	Consultare le procedure fornite nelle guide all'installazione dell'hardware dello switch e nelle istruzioni di installazione e configurazione NetApp .

2. Cablare la rete del cluster e gli switch della rete di gestione ai controller utilizzando il foglio di lavoro di cablaggio compilato, come descritto in ["Foglio di lavoro completo sul cablaggio Cisco Nexus 3132Q-V"](#) .
3. Accendere la rete del cluster e gli switch e i controller della rete di gestione.
4. Eseguire una configurazione iniziale degli switch di rete del cluster.

Fornire risposte pertinenti alle seguenti domande sulla configurazione iniziale al primo avvio dello switch. La politica di sicurezza del tuo sito definisce le risposte e i servizi da abilitare.

Richiesta	Risposta
Interrompere il provisioning automatico e continuare con la configurazione normale? (sì/no)	Rispondi con sì . L'impostazione predefinita è no.
Vuoi applicare uno standard di password sicura? (sì/no)	Rispondi con sì . L'impostazione predefinita è sì.
Inserisci la password per l'amministratore:	La password predefinita è "admin"; è necessario crearne una nuova, più complessa. Una password debole può essere rifiutata.
Desideri accedere alla finestra di dialogo di configurazione di base? (sì/no)	Rispondere con sì alla configurazione iniziale dello switch.
Vuoi creare un altro account di accesso? (sì/no)	La risposta dipende dalle policy del tuo sito relative agli amministratori alternativi. L'impostazione predefinita è no .
Configurare la stringa di comunità SNMP di sola lettura? (sì/no)	Rispondi con no . L'impostazione predefinita è no.

Richiesta	Risposta
Configurare la stringa di comunità SNMP di lettura-scrittura? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Inserisci il nome dello switch.	Il nome dello switch è limitato a 63 caratteri alfanumerici.
Continuare con la configurazione della gestione fuori banda (mgmt0)? (sì/no)	Rispondere con sì (impostazione predefinita) a tale richiesta. Al prompt mgmt0 IPv4 address:, inserisci il tuo indirizzo IP: ip_address.
Configurare il gateway predefinito? (sì/no)	Rispondi con sì . All'indirizzo IPv4 del prompt default-gateway:, immettere default_gateway.
Configurare le opzioni IP avanzate? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Abilitare il servizio telnet? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Servizio SSH abilitato? (sì/no)	Rispondi con sì. L'impostazione predefinita è sì.  Si consiglia di utilizzare SSH quando si utilizza Ethernet Switch Health Monitor (CSHM) per le sue funzionalità di raccolta dei log. Per una maggiore sicurezza si consiglia anche l'uso di SSHv2.
Inserisci il tipo di chiave SSH che vuoi generare (dsa/rsa/rsa1).	Il valore predefinito è rsa .
Inserire il numero di bit della chiave (1024-2048).	Inserisci i bit chiave da 1024 a 2048.
Configurare il server NTP? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Configurare il livello di interfaccia predefinito (L3/L2):	Rispondi con L2 . Il valore predefinito è L2.
Configura lo stato predefinito dell'interfaccia della porta dello switch (shut/noshut):	Rispondi con noshut . L'impostazione predefinita è noshut.
Configurare il profilo del sistema CoPP (rigoroso/moderato/indulgente/de nso):	Rispondi con rigoroso . L'impostazione predefinita è rigorosa.

Richiesta	Risposta
Vuoi modificare la configurazione? (sì/no)	A questo punto dovresti vedere la nuova configurazione. Rivedi e apporta tutte le modifiche necessarie alla configurazione appena inserita. Se sei soddisfatto della configurazione, rispondi no al prompt. Rispondi sì se desideri modificare le impostazioni di configurazione.
Utilizzare questa configurazione e salvarla? (sì/no)	Rispondere con sì per salvare la configurazione. In questo modo vengono aggiornate automaticamente le immagini di kickstart e di sistema.  Se non si salva la configurazione in questa fase, nessuna delle modifiche sarà effettiva al successivo riavvio dello switch.

- Verificare le scelte di configurazione effettuate nella schermata che appare al termine dell'installazione e assicurarsi di salvare la configurazione.
- Controllare la versione sugli switch di rete del cluster e, se necessario, scaricare la versione del software supportata da NetApp sugli switch dal ["Scarica il software Cisco"](#) pagina.

Cosa succederà ora?

Dopo aver configurato gli switch, ["prepararsi a installare NX-OS e RCF"](#).

Prepararsi all'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.

Informazioni sugli esempi

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

Vedi ["Hardware Universe"](#) per verificare le porte cluster corrette sulle tue piattaforme. Vedere ["Quali informazioni aggiuntive mi servono per installare la mia attrezzatura che non è presente in HWU?"](#) per maggiori informazioni sui requisiti di installazione degli switch.



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

Gli esempi in 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 `cluster1-01` e `cluster1-02_clus1` E `cluster1-02_clus2` per `cluster1-02`.
- IL `cluster1::*>` il prompt indica il nome del cluster.

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi degli switch Cisco Nexus serie 3000; salvo diversa indicazione, vengono utilizzati i comandi ONTAP.

Passi

1. Se AutoSupport è abilitato su questo cluster, sopprimere la creazione automatica dei casi 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 avvisa il supporto tecnico di questa attività di manutenzione, in modo che la creazione automatica dei casi venga soppressa durante la finestra di manutenzione.

2. Modificare il livello di privilegio in avanzato, immettendo **y** quando richiesto per continuare:

```
set -privilege advanced
```

Il prompt avanzato(*>) appare.

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. Visualizza gli attributi della porta di rete:

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

Mostra esempio

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

Node: cluster1-02

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

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. Visualizza 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. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

Puoi usare il `network interface check cluster-connectivity` comando per avviare un controllo di accessibilità per la connettività del cluster e quindi visualizzare i dettagli:

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

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

NOTA: attendere alcuni secondi prima di eseguire il comando `show` per visualizzare i dettagli.

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

Packet	Source	Destination
Node Date Loss	LIF	LIF
-----	-----	
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2
none		

Tutte le versioni ONTAP

Per tutte le versioni ONTAP , è anche possibile utilizzare `cluster ping-cluster -node <name>` comando per verificare la connettività:

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

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verificare che il `auto-revert` il comando è abilitato su tutti i 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

Cosa succederà ora?

Dopo esserti preparato per installare il software NX-OS e RCF, ["installare il software NX-OS"](#).

Installa il software NX-OS

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

Requisiti di revisione

Prima di iniziare

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

Documentazione suggerita

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

Installa il software

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi degli switch Cisco Nexus serie 3000; salvo diversa indicazione, vengono utilizzati i comandi ONTAP .

Assicurati di completare la procedura in ["Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento"](#) e poi seguire i passaggi sottostanti.

Passi

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

Mostra esempio

```
cs2# ping 172.19.2.1 vrf management
Ping 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Visualizza le porte del cluster su ciascun nodo connesso 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::*>
```

4. Controllare lo stato amministrativo e operativo di ogni porta del cluster.

a. Verificare che tutte le porte del cluster siano **attive** e in stato di integrità:

```
network port show -role cluster
```

Mostra esempio

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

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

```
network interface show -role Cluster
```

Mostra esempio

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			
8 entries were displayed.				
cluster1::*>				

c. 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                   10.233.205.90    N3K-
C3132Q-V
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network                   10.233.205.91    N3K-
C3132Q-V
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Disabilitare il ripristino automatico sui LIF del cluster. I LIF del cluster eseguono il failover sullo switch del cluster partner e vi rimangono mentre si esegue la procedura di aggiornamento sullo switch di destinazione:

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

6. 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 ["Guida di riferimento ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

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.
```

7. 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#
```

8. Installare l'immagine NX-OS.

L'installazione del file immagine fa sì che questo venga caricato 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#
```

9. 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#
```

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

a. Verificare che le porte del cluster siano attive e funzionanti su tutti i nodi del cluster:

```
network port show -role cluster
```


Mostra esempio

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

8 entries were displayed.

b. Verificare lo stato di integrità dello switch dal 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	

cluster1-01/cdp				
	e0a	cs1	Ethernet1/7	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/7	N3K-
C3132Q-V				
cluster01-2/cdp				
	e0a	cs1	Ethernet1/8	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/8	N3K-
C3132Q-V				
cluster01-3/cdp				
	e0a	cs1	Ethernet1/1/1	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/1	N3K-
C3132Q-V				
cluster1-04/cdp				
	e0a	cs1	Ethernet1/1/2	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/2	N3K-
C3132Q-V				

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

Switch Model	Type	Address	

cs1	cluster-network	10.233.205.90	N3K-
C3132Q-V			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N3K-

```

C3132Q-V
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

A seconda della versione RCF precedentemente caricata sullo switch, è possibile che venga visualizzato il seguente output sulla console dello switch cs1:

```

2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.

```

11. Verificare che il cluster sia integro:

```
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::*>

```

12. Ripetere i passaggi da 6 a 11 sullo switch cs1.

13. Abilita il ripristino automatico sui LIF del cluster.

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

14. Verificare che i LIF del cluster siano tornati alla loro porta home:

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

Mostra esempio

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		
8 entries were displayed.				
cluster1::*>				

Se alcuni LIF del cluster non sono tornati alle loro porte home, ripristinarli manualmente dal nodo locale:

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

Cosa succederà ora?

Dopo aver installato il software NX-OS, puoi ["installare o aggiornare il file di configurazione di riferimento \(RCF\)"](#).

Installare o aggiornare l'RCF

Panoramica sull'installazione o l'aggiornamento del file di configurazione di riferimento (RCF)

Dopo aver configurato per la prima volta gli switch Nexus 3132Q-V, installare il file di configurazione di riferimento (RCF). È possibile aggiornare la versione RCF quando sullo switch è installata una versione esistente del file RCF.

Vedi l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Cisco mantenendo la connettività remota"](#) per ulteriori informazioni sull'installazione o l'aggiornamento del tuo RCF.

Configurazioni RCF disponibili

Nella tabella seguente vengono descritti gli RCF disponibili per diverse configurazioni. Scegli l'RCF applicabile alla tua configurazione.

Per informazioni specifiche sull'utilizzo di porte e VLAN, fare riferimento alla sezione banner e note importanti nel RCF.

Nome RCF	Descrizione
Breakout di 2 cluster HA	Supporta due cluster ONTAP con almeno otto nodi, inclusi i nodi che utilizzano porte Cluster+HA condivise.
Breakout di 4 cluster HA	Supporta quattro cluster ONTAP con almeno quattro nodi, inclusi i nodi che utilizzano porte Cluster+HA condivise.
1-Cluster-HA	Tutte le porte sono configurate per 40/100GbE. Supporta il traffico cluster/HA condiviso sulle porte. Richiesto per i sistemi AFF A320, AFF A250 e FAS500f . Inoltre, tutte le porte possono essere utilizzate come porte cluster dedicate.
1-Cluster-HA-Breakout	Le porte sono configurate per breakout 4x10GbE, breakout 4x25GbE (RCF 1.6+ su switch 100GbE) e 40/100GbE. Supporta il traffico cluster/HA condiviso sulle porte per i nodi che utilizzano porte cluster/HA condivise: sistemi AFF A320, AFF A250 e FAS500f . Inoltre, tutte le porte possono essere utilizzate come porte cluster dedicate.
Cluster-HA-Storage	Le porte sono configurate per 40/100 GbE per Cluster+HA, breakout 4x10 GbE per Cluster e breakout 4x25 GbE per Cluster+HA e 100 GbE per ogni coppia Storage HA.
Grappolo	Due tipi di RCF con diverse allocazioni di 4 porte 10GbE (breakout) e porte 40/100GbE. Sono supportati tutti i nodi FAS/ AFF , ad eccezione dei sistemi AFF A320, AFF A250 e FAS500f .
Magazzinaggio	Tutte le porte sono configurate per connessioni di archiviazione NVMe da 100 GbE.

RCF disponibili

Nella tabella seguente sono elencati gli RCF disponibili per gli switch 3132Q-V. Scegli la versione RCF

applicabile alla tua configurazione. Vedere ["Switch Ethernet Cisco"](#) per maggiori informazioni.

Nome RCF
Cluster-HA-Breakout RCF v1.xx
Cluster-HA RCF v1.xx
Gruppo RCF 1.xx

Documentazione suggerita

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

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate sul sito di supporto NetApp . Si noti che possono esserci dipendenze tra la sintassi dei comandi nella RCF e la sintassi presente in versioni specifiche di NX-OS.

- ["Switch Cisco Nexus serie 3000"](#)

Per la documentazione completa sulle procedure di upgrade e downgrade degli switch Cisco , fare riferimento alle guide software e di aggiornamento appropriate disponibili sul sito Web Cisco .

Informazioni sugli esempi

Gli esempi in 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::*>` il prompt indica il nome del cluster.

Gli esempi in questa procedura utilizzano quattro nodi. Questi nodi utilizzano due porte di interconnessione cluster 10GbE **e0a** e **e0b**. Vedi il ["Hardware Universe"](#) per verificare le porte cluster corrette sulle tue piattaforme.



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

Per i dettagli delle configurazioni RCF disponibili, vedere ["Flusso di lavoro di installazione del software"](#) .

Comandi utilizzati

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi degli switch Cisco Nexus serie 3000; salvo diversa indicazione, vengono utilizzati i comandi ONTAP .

Cosa succederà ora?

Dopo aver esaminato la procedura di installazione o aggiornamento RCF, è possibile ["installare l'RCF"](#) O ["aggiorna il tuo RCF"](#) come richiesto.

Installare il file di configurazione di riferimento (RCF)

Dopo aver configurato per la prima volta gli switch Nexus 3132Q-V, installare il file di configurazione di riferimento (RCF).

Prima di iniziare

Verificare le seguenti installazioni e connessioni:

- Un backup attuale della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- L'attuale RCF.
- Una connessione della console allo switch, necessaria durante l'installazione dell'RCF.

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi degli switch Cisco Nexus serie 3000; salvo diversa indicazione, vengono utilizzati i comandi ONTAP .

Durante questa procedura non è necessario alcun collegamento inter-switch (ISL) operativo. Ciò è voluto perché le modifiche alla versione RCF possono influire temporaneamente sulla connettività ISL. Per abilitare operazioni cluster senza interruzioni, la seguente procedura migra tutti i LIF del cluster allo switch partner operativo, eseguendo al contempo i passaggi sullo switch di destinazione.

Fase 1: installare l'RCF sugli switch

1. Visualizza le porte del cluster su ciascun nodo connesso 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 ogni porta del cluster.

a. Verificare che tutte le porte del cluster siano attive e integre:

```
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
```

Speed (Mbps)

```

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

```

b. Verificare che tutte le interfacce cluster (LIF) siano sulla 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 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. Disabilitare il ripristino automatico sui LIF del cluster.

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

Dopo aver eseguito questo comando, assicurarsi che il ripristino automatico sia disabilitato.

4. Sullo switch del cluster cs2, chiudere le porte connesse alle porte del cluster dei nodi.

```

cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



Il numero di porte visualizzate varia in base al numero di nodi nel cluster.

- Verificare che le porte del cluster siano state sottoposte a failover sulle porte ospitate sullo switch del cluster cs1. Potrebbero volerci 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::*>				

- Verificare che il cluster sia integro:

```
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::*>
```

7. Se non lo hai già fatto, salva una copia della configurazione corrente dello switch copiando l'output del seguente comando in un file di testo:

```
show running-config
```

8. Registrare eventuali aggiunte personalizzate tra il file running-config corrente e il file RCF in uso.



Assicurati di configurare quanto segue: * Nome utente e password * Indirizzo IP di gestione
* Gateway predefinito * Nome dello switch

9. Salva i dettagli di configurazione di base nel `write_erase.cfg` file sul bootflash.



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 connessi alla porta della console seriale.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

10. Quando si installa RCF versione 1.12 e successive, eseguire i seguenti comandi:

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>
```

```
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>  
bootflash:write_erase.cfg
```

Vedi l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Cisco mantenendo la connettività remota"](#) per ulteriori dettagli.

11. Verificare che il `write_erase.cfg` il file è popolato come previsto:

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

12. Emettere il `write erase` comando per cancellare la configurazione salvata corrente:

```
cs2# write erase
```

```
Warning: This command will erase the startup-configuration.
```

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

13. Copiare la configurazione di base salvata in precedenza nella configurazione di avvio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

14. Riavviare lo switch:

```
cs2# reload
```

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

15. Ripetere i passaggi da 7 a 14 sullo switch cs1.

16. Collegare le porte del cluster di tutti i nodi nel cluster ONTAP agli switch cs1 e cs2.

Passaggio 2: verificare le connessioni dello switch

1. Verificare che le porte dello switch collegate alle porte del cluster siano **attive**.

```
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 sia funzionante:

```
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 i LIF del cluster siano tornati alla loro 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 sia integro:

```
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::*>
```

Passaggio 3: configura il tuo cluster ONTAP

NetApp consiglia di utilizzare System Manager per configurare nuovi cluster.

System Manager fornisce un flusso di lavoro semplice e facile per l'impostazione e la configurazione del cluster, tra cui l'assegnazione di un indirizzo IP di gestione del nodo, l'inizializzazione del cluster, la creazione di un livello locale, la configurazione dei protocolli e il provisioning dello storage iniziale.

Fare riferimento a ["Configurare ONTAP su un nuovo cluster con System Manager"](#) per le istruzioni di installazione.

Cosa succederà ora?

Dopo aver installato l'RCF, puoi ["verificare la configurazione SSH"](#).

Aggiorna il tuo file di configurazione di riferimento (RCF)

È possibile aggiornare la versione RCF quando è installata una versione esistente del file RCF sugli switch operativi.

Prima di iniziare

Assicurati di avere quanto segue:

- Un backup attuale della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- L'attuale RCF.
- Se si aggiorna la versione RCF, è necessaria una configurazione di avvio in RCF che rifletta le immagini di avvio desiderate.

Se è necessario modificare la configurazione di avvio per riflettere le immagini di avvio correnti, è necessario farlo prima di riapplicare l'RCF, in modo che ai riavvii futuri venga istanziata la versione corretta.



Durante questa procedura non è necessario alcun collegamento inter-switch (ISL) operativo. Ciò è voluto perché le modifiche alla versione RCF possono influire temporaneamente sulla connettività ISL. Per garantire operazioni del cluster senza interruzioni, la seguente procedura migra tutti i LIF del cluster allo switch partner operativo, eseguendo al contempo i passaggi sullo switch di destinazione.



Prima di installare una nuova versione del software dello switch e degli RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. È necessario essere connessi allo switch tramite la console seriale oppure aver conservato le informazioni di configurazione di base prima di cancellare le impostazioni dello switch.

Passaggio 1: Prepararsi all'aggiornamento

1. Visualizza le porte del cluster su ciascun nodo connesso 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 ogni porta del cluster.

a. Verificare che tutte le porte del cluster siano attive e integre:

```
network port show -ip space 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 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. Disabilitare il ripristino automatico sui LIF del cluster.

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

Dopo aver eseguito questo comando, assicurarsi che il ripristino automatico sia disabilitato.

Passaggio 2: configurare le porte

1. Sullo switch del cluster cs2, chiudere le porte connesse alle porte del cluster dei nodi.

```

cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



Il numero di porte visualizzate varia in base al numero di nodi nel cluster.

2. Verificare che le porte del cluster siano state sottoposte a failover sulle porte ospitate sullo switch del cluster cs1. Potrebbero volerci alcuni secondi.

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

3. Verificare che il cluster sia integro:


```
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::*>
```

4. Se non lo hai già fatto, salva una copia della configurazione corrente dello switch copiando l'output del seguente comando in un file di testo:

```
show running-config
```

5. Registrare eventuali aggiunte personalizzate tra il file running-config corrente e il file RCF in uso.

Assicurati di configurare quanto segue:



- Nome utente e password
- Indirizzo IP di gestione
- Gateway predefinito
- Cambia nome

6. Salva i dettagli di configurazione di base nel `write_erase.cfg` file sul bootflash.



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

7. Quando si esegue l'aggiornamento alla versione RCF 1.12 e successive, eseguire i seguenti comandi:

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>
bootflash:write_erase.cfg

cs2# echo "hardware access-list tcam region e-racl 256" >>
bootflash:write_erase.cfg

cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

8. Verificare che il `write_erase.cfg` il file è popolato come previsto:

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

9. Emettere il `write erase` comando per cancellare la configurazione salvata corrente:

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

10. Copiare la configurazione di base salvata in precedenza nella configurazione di avvio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Riavviare lo switch:

```
cs2# reload
```

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

12. Una volta che l'indirizzo IP di gestione è nuovamente raggiungibile, accedere allo switch tramite SSH.

Potrebbe essere necessario aggiornare le voci del file host relative alle chiavi SSH.

13. Copiare l'RCF nel bootflash 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 nel "[Riferimento ai comandi NX-OS della serie Cisco Nexus 3000](#)" 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)...
```

14. Applicare l'RCF precedentemente scaricato al bootflash.

Per ulteriori informazioni sui comandi Cisco , consultare la guida appropriata nel ["Riferimento ai comandi NX-OS della serie Cisco Nexus 3000"](#) guide.

Mostra esempio

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



Assicuratevi di leggere attentamente le sezioni **Note di installazione**, **Note importanti** e **banner** del vostro RCF. Per garantire la corretta configurazione e il corretto funzionamento dello switch, è necessario leggere e seguire queste istruzioni.

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

```
show running-config
```

Quando controllate l'output per verificare di avere l'RCF corretto, assicurati che le seguenti informazioni siano corrette:

- Lo striscione RCF
- Le impostazioni del nodo e della 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 i passaggi su come portare online le porte 10GbE dopo un aggiornamento dell'RCF, consultare l'articolo della Knowledge Base ["Le porte 10GbE su uno switch cluster Cisco 3132Q non sono online"](#) .

16. Dopo aver verificato che le versioni RCF e le impostazioni degli switch siano corrette, copiare il file running-config file al startup-config file.

Per ulteriori informazioni sui comandi Cisco , consultare la guida appropriata nel ["Riferimento ai comandi NX-OS della serie Cisco Nexus 3000"](#) guide.

Mostra esempio

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

17. Riavviare lo switch cs2. È possibile ignorare sia gli eventi "porte cluster inattive" segnalati sui nodi mentre lo switch si riavvia sia l'errore % Invalid command at '^' marker produzione.

```
cs2# reload
```

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

18. Riapplicare eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a ["Esaminare le considerazioni sul cablaggio e sulla configurazione"](#) per i dettagli di eventuali ulteriori modifiche richieste.
19. Verificare lo stato delle porte del cluster sul cluster.
 - a. Verificare che le porte del cluster siano attive e funzionanti su 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 di integrità 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, è possibile che venga visualizzato il seguente output sulla console dello switch cs1:



```

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.

```

+



Possono essere necessari fino a 5 minuti prima che i nodi del cluster vengano segnalati come integri.

20. Sullo switch del cluster cs1, chiudere le porte collegate alle porte del cluster dei nodi.

Mostra esempio

```

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

```



Il numero di porte visualizzate varia in base al numero di nodi nel cluster.

21. Verificare che i LIF del cluster siano stati migrati alle porte ospitate sullo switch cs2. Potrebbero volerci 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::*>				

22. Verificare che il cluster sia integro:

```
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::*>
```

23. Ripetere i passaggi da 1 a 19 sullo switch cs1.

24. Abilita il ripristino automatico sui LIF del cluster.

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

25. Riavviare l'interruttore cs1. In questo modo si attiva il ripristino dei LIF del cluster alle rispettive porte home. È possibile ignorare gli eventi "porte cluster inattive" segnalati sui nodi mentre lo switch si riavvia.

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

Passaggio 3: verificare la configurazione

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

```
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 sia funzionante:

```
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 i LIF del cluster siano tornati alle loro porte 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 sia integro:

```
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. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

Puoi usare il `network interface check cluster-connectivity` comando per avviare un controllo di accessibilità per la connettività del cluster e quindi visualizzare i dettagli:

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

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

NOTA: attendere alcuni secondi prima di eseguire il comando `show` per visualizzare i dettagli.

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

Packet	Source	Destination
Node Date Loss	LIF	LIF
-----	-----	
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2
none		

Tutte le versioni ONTAP

Per tutte le versioni ONTAP , è anche possibile utilizzare `cluster ping-cluster -node <name>` comando per verificare la connettività:

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

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status: .....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

Cosa succederà ora?

Dopo aver aggiornato il tuo RCF, ["verificare la configurazione SSH"](#) .

Verifica la tua configurazione SSH

Se si utilizzano le funzionalità di monitoraggio dello stato dello switch Ethernet (CSHM) e di raccolta dei registri, verificare che SSH e le chiavi SSH siano abilitati sugli switch del cluster.

Passi

1. Verificare che SSH sia abilitato:

```

(switch) show ssh server
ssh version 2 is enabled

```

2. Verificare che le chiavi SSH siano abilitate:

```
show ssh key
```

Mostra esempio

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlIoC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

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



Quando si abilita FIPS, è necessario modificare il bitcount a 256 sullo switch utilizzando il comando `ssh key ecdsa 256 force`. Vedere ["Configurare la sicurezza di rete utilizzando FIPS"](#) per maggiori dettagli.

Cosa succederà ora?

Dopo aver verificato la configurazione SSH, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Ripristinare lo switch del cluster 3132Q-V ai valori predefiniti di fabbrica

Per ripristinare le impostazioni predefinite di fabbrica dello switch cluster 3132Q-V, è necessario cancellare le impostazioni dello switch 3132Q-V.

Informazioni su questo compito

- È necessario connettersi allo switch tramite la console seriale.
- Questa attività reimposta la configurazione della rete di gestione.

Passi

1. Cancella la configurazione esistente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Ricaricare il software dello switch:

```
reload
```

```
(cs2)# reload
```

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

Il sistema si riavvia e accede alla procedura guidata di configurazione. Durante l'avvio, se viene visualizzato il messaggio "Interrompere il provisioning automatico e continuare con la configurazione normale?" (sì/no)[n]", dovresti rispondere **sì** per procedere.

Cosa c'è dopo?

Dopo aver ripristinato l'interruttore, è possibile ["riconfigurare"](#) in base alle tue esigenze.

Informazioni sul copyright

Copyright © 2026 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.