



Configurare il software

Install and maintain

NetApp
January 30, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems-switches/switch-cisco-9336c-fx2/configure-software-overview-9336c-cluster.html> on January 30, 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 9336C-FX2 e 9336C-FX2-T 1
 - Configurare gli switch cluster 9336C-FX2 e 9336C-FX2-T 1
 - Prepararsi all'installazione del software NX-OS e RCF 4
 - Installa o aggiorna il software NX-OS 11
 - Requisiti di revisione 11
 - Installa il software 12
 - Installare o aggiornare l'RCF 34
 - Panoramica sull'installazione o l'aggiornamento del file di configurazione di riferimento (RCF) 34
 - Installare il file di configurazione di riferimento (RCF) 36
 - Aggiorna il tuo file di configurazione di riferimento (RCF) 45
 - Verifica la tua configurazione SSH 70
 - Ripristinare i valori predefiniti di fabbrica degli switch cluster 9336C-FX2 e 9336C-FX2-T 73

Configurare il software

Flusso di lavoro di installazione del software per gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per installare e configurare il software per gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T e per installare o aggiornare il file di configurazione di riferimento (RCF), attenersi alla seguente procedura:

1

"Configurare l'interruttore"

Configurare gli switch cluster 9336C-FX2 e 9336C-FX2-T.

2

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

Il software Cisco NX-OS e i file di configurazione di riferimento (RCF) devono essere installati sugli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T.

3

"Installa o aggiorna il software NX-OS"

Scarica e installa o aggiorna il software NX-OS sugli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T.

4

"Installare o aggiornare l'RCF"

Installare o aggiornare l'RCF dopo aver configurato per la prima volta gli switch Cisco 9336C-FX2 e 9336C-FX2-T. Puoi usare questa procedura anche per aggiornare la tua versione RCF.

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 degli switch cluster 9336C-FX2 e 9336C-FX2-T.

Configurare gli switch cluster 9336C-FX2 e 9336C-FX2-T

Seguire questa procedura per configurare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Prima di iniziare

Assicurati di avere quanto segue:

- 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.
- Licenze applicabili, informazioni di rete e configurazione e cavi.
- Completato ["fogli di lavoro sul cablaggio"](#) .
- RCF applicabili alla rete cluster NetApp e alla rete di gestione scaricabili dal sito di supporto NetApp all'indirizzo ["mysupport.netapp.com"](#) . 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.
- ["Documentazione richiesta per switch e ONTAP"](#).

Passi

1. 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.
Configurare la stringa di comunità SNMP di lettura-scrittura? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Inserisci il nome dello switch.	Immettere il nome dello switch, che 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.

Richiesta	Risposta
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 il numero di bit della 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.
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.

Richiesta	Risposta
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.

2. Verificare le scelte di configurazione effettuate nella schermata che appare al termine dell'installazione e assicurarsi di salvare la configurazione.
3. 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, puoi ["prepararsi a installare il software NX-OS e RCF"](#).

Prepararsi all'installazione del software NX-OS e RCF

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

Documentazione suggerita

- ["Pagina dello switch Ethernet Cisco"](#)

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e NX-OS supportate.

- ["Guide per l'aggiornamento e il downgrade del software"](#)

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 .

- ["Aggiornamento Cisco Nexus 9000 e 3000 e matrice ISSU"](#)

Fornisce informazioni sull'aggiornamento/downgrade dirompente per il software Cisco NX-OS sugli switch Nexus serie 9000 in base alle versioni correnti e di destinazione.

Nella pagina, seleziona **Disruptive Upgrade** e seleziona la versione corrente e quella di destinazione dall'elenco a discesa.

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 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 9000; 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=x h`

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	N9K-
C9336C	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/cdp	e0a	cs1	Eth1/1	N9K-
C9336C	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

4. Controllare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.
 - a. Visualizza gli attributi della porta di rete:

```
network port show -ip space Cluster
```


Mostra esempio

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

```
Node: cluster1-02
```

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

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

```
Node: cluster1-01
```

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

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

```
4 entries were displayed.
```

b. Visualizza informazioni sui LIF:

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

Mostra esempio

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.49.125/16	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			

4 entries were displayed.

5. Verificare la connettività delle interfacce del cluster remoto:

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:

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

```

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

```

				Source	Destination
Packet					
Node	Date			LIF	LIF
Loss					
-----	-----			-----	
-----	-----				
node1					
	3/5/2022	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				
node2					
	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				

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

9

```

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 comando di ripristino automatico sia 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

4 entries were displayed.

Cosa succederà ora?

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

Installa o aggiorna il software NX-OS

Seguire questa procedura per installare o aggiornare il software NX-OS sugli switch cluster Nexus 9336C-FX2 e 9336C-FX2-T.

Prima di iniziare, completare la procedura in ["Prepararsi all'installazione di NX-OS e RCF"](#).

Requisiti di revisione

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).

Documentazione suggerita

- ["Pagina dello switch Ethernet Cisco"](#)

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e NX-OS supportate.

- ["Guide per l'aggiornamento e il downgrade del software"](#)

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.

- ["Aggiornamento Cisco Nexus 9000 e 3000 e matrice ISSU"](#)

Fornisce informazioni sull'aggiornamento/downgrade dirompente per il software Cisco NX-OS sugli switch

Nexus serie 9000 in base alle versioni correnti e di destinazione.

Nella pagina, seleziona **Disruptive Upgrade** e seleziona la versione corrente e quella di destinazione dall'elenco a discesa.

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 dei 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.

Installa il software

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi degli switch Cisco Nexus serie 9000; salvo diversa indicazione, vengono utilizzati i comandi ONTAP .

Passi

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

Mostra esempio

Questo esempio verifica che lo switch possa raggiungere il server all'indirizzo IP 172.19.2.1:

```
cs2# ping 172.19.2.1 VRF management
Pinging 172.19.2.1 with 0 bytes of data:

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

3. 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      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

4. 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
```

	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			
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      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network     10.233.205.91      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. 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 e le immagini EPLD sullo switch Nexus 9336C-FX2.

Mostra esempio

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. 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 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. 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.9.3.5.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Performing module support checks.  
[] 100% -- SUCCESS
```

```
Notifying services about system upgrade.  
[] 100% -- SUCCESS
```

Compatibility check is done:

Module	Bootable	Impact	Install-type	Reason
1	yes	Disruptive	Reset	Default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-
Version		Upg-Required	
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		yes	

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

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

```
show version
```



```
cs2# show version
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
```

Software

```
BIOS: version 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
cisco Nexus9000 C9336C-FX2 Chassis
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
Processor Board ID FOC20291J6K

Device name: cs2
bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

10. Aggiornare l'immagine EPLD e riavviare lo switch.

Mostra esempio



```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x17
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Dopo il riavvio dello switch, effettuare nuovamente l'accesso e verificare che la nuova versione di EPLD sia stata caricata correttamente.

Mostra esempio

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

12. 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	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.

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	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

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

Switch Model	Type	Address	

cs1 C9336C-FX2	cluster-network	10.233.205.90	N9K-
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-


```

C9336C-FX2
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

13. 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::*>

```

14. Ripetere i passaggi da 6 a 13 per installare il software NX-OS sullo switch cs1.

15. Verificare la connettività delle interfacce del cluster remoto prima di abilitare il ripristino automatico sui LIF del cluster:

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:

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

```

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

```

				Source	Destination
Packet					
Node	Date			LIF	LIF
Loss					
-----	-----	-----	-----	-----	-----
node1	3/5/2022	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				
node2					
	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				

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

32

```

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. Abilita il ripristino automatico sui LIF del cluster.

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

2. 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 o aggiornato 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 9336C-FX2 e 9336C-FX2-T, 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. Vedere ["Switch Ethernet Cisco"](#) per maggiori informazioni.

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

Configurazione 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 9336C-FX2 e 9336C-FX2-T. Scegli la versione RCF applicabile alla tua configurazione. Vedere ["Switch Ethernet Cisco"](#) per maggiori informazioni.

Nome RCF
Cluster-HA-Breakout RCF 1.xx

Nome RCF
Cluster-HA-Storage RCF 1.xx
RCF di stoccaggio 1.xx
MultiCluster-HA 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 9000"](#)

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 9000; 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 9336C-FX2 e 9336C-FX2-T, installare il file di configurazione di riferimento (RCF).

Prima di iniziare

Verificare le seguenti installazioni e connessioni:

- Una connessione della console allo switch. La connessione alla console è facoltativa se si ha accesso remoto allo switch.
- Gli switch cs1 e cs2 vengono accesi e la configurazione iniziale dello switch è completata (l'indirizzo IP di gestione e SSH sono configurati).
- La versione NX-OS desiderata è stata installata.
- Le connessioni ISL tra gli switch sono connesse.
- Le porte del cluster del nodo ONTAP non sono connesse.

Fase 1: installare l'RCF sugli switch

1. Accedi per cambiare cs1 tramite SSH o tramite una console seriale.
2. Copiare l'RCF nel bootflash dello switch cs1 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 9000](#)" guide.

Mostra esempio

Questo esempio mostra come TFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_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)...
```

3. 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 9000](#)" guide.

Questo esempio mostra il file RCF Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt in fase di installazione sullo switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```

4. Esaminare l'output del banner dal `show banner motd` comando. Per garantire la corretta configurazione e il corretto funzionamento dello switch, è necessario leggere e seguire queste istruzioni.

Mostra esempio

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

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

```
show running-config
```


Quando controlli 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.

6. Registrare eventuali aggiunte personalizzate tra l'attuale `running-config` file e il file RCF in uso.
7. Dopo aver verificato che le versioni RCF e le impostazioni degli switch siano corrette, copiare il file `running-config` file al `startup-config` file.

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

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

Assicurati di configurare quanto segue:



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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

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

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

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

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

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

11. Ripetere i passaggi da 1 a 10 sullo switch cs2.

12. 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
```

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 i nodi del cluster si trovino nelle VLAN del cluster corrette utilizzando i seguenti comandi:

```
show vlan brief
```

```
show interface trunk
```

Mostra esempio

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/35, Eth1/36, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15, Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

```

-----
Port                Native  Status      Port
                   Vlan                                Channel
-----
Eth1/1              1      trunking    --
Eth1/2              1      trunking    --
Eth1/3              1      trunking    --
Eth1/4              1      trunking    --
Eth1/5              1      trunking    --
Eth1/6              1      trunking    --
Eth1/7              1      trunking    --
Eth1/8              1      trunking    --
Eth1/9/1            1      trunking    --
Eth1/9/2            1      trunking    --
Eth1/9/3            1      trunking    --
Eth1/9/4            1      trunking    --
Eth1/10/1           1      trunking    --
Eth1/10/2           1      trunking    --
Eth1/10/3           1      trunking    --
Eth1/10/4           1      trunking    --
Eth1/11             33     trunking    --

```

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

```

-----
Port                Vlans Allowed on Trunk
-----
Eth1/1              1,17-18
Eth1/2              1,17-18
Eth1/3              1,17-18
Eth1/4              1,17-18
Eth1/5              1,17-18
Eth1/6              1,17-18
Eth1/7              1,17-18
Eth1/8              1,17-18
Eth1/9/1            1,17-18
Eth1/9/2            1,17-18
Eth1/9/3            1,17-18
Eth1/9/4            1,17-18
Eth1/10/1           1,17-18
Eth1/10/2           1,17-18
Eth1/10/3           1,17-18
Eth1/10/4           1,17-18

```

```
Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..
```



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

3. 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      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

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.

Vai 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      N9K-
C9336C
           e0d    cs2                      Ethernet1/7      N9K-
C9336C
cluster1-02/cdp
           e0a    cs1                      Ethernet1/8      N9K-
C9336C
           e0d    cs2                      Ethernet1/8      N9K-
C9336C
cluster1-03/cdp
           e0a    cs1                      Ethernet1/1/1    N9K-
C9336C
           e0b    cs2                      Ethernet1/1/1    N9K-
C9336C
cluster1-04/cdp
           e0a    cs1                      Ethernet1/1/2    N9K-
C9336C
           e0b    cs2                      Ethernet1/1/2    N9K-
C9336C
cluster1::*>
```

2. 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 -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			
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      N9K-
C9336C
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network     10.233.205.91      N9K-
C9336C
    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::*>
```

3. Disabilitare il ripristino automatico sui LIF del cluster.

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

Passaggio 2: configurare le porte

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

```
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
```



Assicurarsi di chiudere **tutte** le porte del cluster connesse per evitare problemi di connessione di rete. Vedi l'articolo della Knowledge Base ["Nodo fuori quorum durante la migrazione del cluster LIF durante l'aggiornamento del sistema operativo dello switch"](#) per ulteriori dettagli.

2. Verificare che i LIF del cluster abbiano eseguito il 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			
8 entries were displayed.				
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
4 entries were displayed.
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
```

- Registrazione eventuali aggiunte personalizzate tra l'attuale `running-config` e il file RCF in uso (ad esempio una configurazione SNMP per la tua organizzazione).
 - A partire da NX-OS 10.2, utilizzare `show diff running-config` comando per confrontare con il file RCF salvato nel bootflash. In caso contrario, utilizzare uno strumento di confronto/differenza di terze parti.
5. Salva i dettagli di configurazione di base nel `write_erase.cfg` file sul bootflash.

Assicurati di configurare quanto segue:



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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

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

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

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

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

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

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

```
cs1# write erase
```

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

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

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

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

10. Eseguire un riavvio dello switch:

```
switch# reload
```

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

11. 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.

12. Copiare l'RCF nel bootflash dello switch cs1 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 9000"](#) guide.

Questo esempio mostra come TFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_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)...
```

13. 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 9000"](#) .

Questo esempio mostra il file RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` in fase di installazione sullo switch `cs1`:

```
cs1# copy Nexus_9336C_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.

14. 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, assicuratevi 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.

15. 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.
16. Dopo aver verificato che le versioni RCF, le aggiunte personalizzate e le impostazioni degli switch siano corrette, copiare il file `running-config` nel file `startup-config`.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata nel ["Riferimento ai comandi NX-OS della serie Cisco Nexus 9000"](#).

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

17. Riavviare l'interruttore `cs1`. È possibile ignorare gli avvisi "monitoraggio integrità switch cluster" e gli eventi "porte cluster inattive" segnalati sui nodi durante il riavvio dello switch.

```
cs1# reload
```

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

18. 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 -ip space cluster
```

Mostra esempio

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

Node: cluster1-01

Ignore

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

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

Node: cluster1-02

Ignore

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

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

Node: cluster1-03

Ignore

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

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

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
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	N9K-
C9336C	e0d	cs2	Ethernet1/7	N9K-
C9336C				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C	e0d	cs2	Ethernet1/8	N9K-
C9336C				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C	e0b	cs2	Ethernet1/1/1	N9K-
C9336C				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C	e0b	cs2	Ethernet1/1/2	N9K-
C9336C				

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

Switch Model	Type	Address	
cs1	cluster-network	10.233.205.90	NX9-
C9336C			
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	NX9-

```

C9336C
  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.

```

19. 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::*>

```

20. Ripetere i passaggi da 1 a 19 sullo switch cs2.

21. Abilita il ripristino automatico sui LIF del cluster.

```

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

```

22. Eseguire un riavvio di switch cs2.

```
cs2# reload
```

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

Passaggio 3: verificare la configurazione della rete del cluster e lo stato del cluster

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

```
show interface brief
```

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 i nodi previsti siano ancora connessi:

```
show cdp neighbors
```

Mostra esempio

```
cs1# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. Verificare che i nodi del cluster si trovino nelle VLAN del cluster corrette utilizzando i seguenti comandi:

```
show vlan brief
```

```
show interface trunk
```

Mostra esempio

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po1, Eth1/1, Eth1/2, Eth1/3 Eth1/4, Eth1/5, Eth1/6, Eth1/7 Eth1/8, Eth1/35, Eth1/36 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13 Eth1/14, Eth1/15, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25


```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active
Eth1/25
Eth1/28
Eth1/31
Eth1/34
Eth1/26, Eth1/27,
Eth1/29, Eth1/30,
Eth1/32, Eth1/33,
Eth1/11, Eth1/12,
Eth1/14, Eth1/15,
Eth1/17, Eth1/18,
Eth1/20, Eth1/21,
Eth1/23, Eth1/24,
Eth1/26, Eth1/27,
Eth1/29, Eth1/30,
Eth1/32, Eth1/33,

```

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	1	trunking	--
Eth1/9/2	1	trunking	--
Eth1/9/3	1	trunking	--
Eth1/9/4	1	trunking	--
Eth1/10/1	1	trunking	--
Eth1/10/2	1	trunking	--
Eth1/10/3	1	trunking	--
Eth1/10/4	1	trunking	--
Eth1/11	33	trunking	--

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

```

-----
Port                Vlans Allowed on Trunk
-----
Eth1/1              1,17-18
Eth1/2              1,17-18
Eth1/3              1,17-18
Eth1/4              1,17-18
Eth1/5              1,17-18
Eth1/6              1,17-18
Eth1/7              1,17-18
Eth1/8              1,17-18
Eth1/9/1            1,17-18
Eth1/9/2            1,17-18
Eth1/9/3            1,17-18
Eth1/9/4            1,17-18
Eth1/10/1           1,17-18
Eth1/10/2           1,17-18
Eth1/10/3           1,17-18
Eth1/10/4           1,17-18

```

```
Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..
```



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

4. 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      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

5. 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		
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 vservice_name -lif lif_name
```

6. 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::*>
```

7. 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 `show` comando per visualizzare i dettagli.

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

Packet	Source	Destination
Node	Date	LIF
Loss		

node1		
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		
node2		
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 cluster1-03
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)

```

Cosa succederà ora?

Dopo aver aggiornato il tuo RCF, puoi [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 i valori predefiniti di fabbrica degli switch cluster 9336C-FX2 e 9336C-FX2-T

Per ripristinare le impostazioni predefinite di fabbrica degli switch cluster 9336C-FX2 e 9336C-FX2-T, è necessario cancellare le impostazioni degli switch 9336C-FX2 e 9336C-FX2-T.

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 gli switch, puoi ["riconfigurare"](#) secondo necessità.

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.