



Interruttori a grappolo

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems-switches/switch-bes-53248/configure-new-switch-overview.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommario

- Interruttori a grappolo 1
 - BES-53248 supportato da Broadcom 1
 - Iniziare 1
 - Installare l'hardware 5
 - Configurare il software 8
 - Aggiorna lo switch 106
 - Migrare gli switch 150
 - Sostituire gli interruttori 188
 - Cisco Nexus 9336C-FX2 o 9336C-FX2-T 216
 - Iniziare 216
 - Installare l'hardware 222
 - Configurare il software 233
 - Migrare gli switch 305
 - Sostituire gli interruttori 360
 - NVIDIA SN2100 392
 - Iniziare 392
 - Installare l'hardware 395
 - Configurare il software 404
 - Migrare gli switch 481
 - Sostituire gli interruttori 539

Interruttori a grappolo

BES-53248 supportato da Broadcom

Iniziare

Flusso di lavoro di installazione e configurazione per gli switch BES-53248

Il BES-53248 è uno switch bare metal progettato per funzionare in cluster ONTAP da due a 24 nodi.

Seguire questi passaggi del flusso di lavoro per installare e configurare gli switch BES-53248.

1

"Rivedere i requisiti di configurazione"

Esaminare i requisiti di configurazione per lo switch cluster BES-53248.

2

"Rivedere i componenti e i numeri delle parti"

Esaminare i componenti e i codici articolo dello switch cluster BES-53248.

3

"Esaminare la documentazione richiesta"

Consultare la documentazione specifica dello switch e del controller per configurare gli switch BES-53248 e il cluster ONTAP .

4

"Installare l'hardware"

Installare l'hardware dello switch.

5

"Configurare il software"

Configurare il software dello switch.

Requisiti di configurazione per gli switch cluster BES-53248

Per l'installazione e la manutenzione dello switch BES-53248, assicurarsi di rivedere i requisiti di supporto e configurazione EFOS e ONTAP .

Supporto EFOS e ONTAP

Vedi il ["Hardware Universe NetApp"](#) E ["Matrice di compatibilità degli switch Broadcom"](#) per informazioni sulla compatibilità EFOS e ONTAP con gli switch BES-53248. Il supporto EFOS e ONTAP può variare in base al tipo di macchina specifico dello switch BES-53248. Per i dettagli di tutti i tipi di macchine di commutazione BES-52348, vedere ["Componenti e numeri di parte per gli switch cluster BES-53248"](#) . Vedere ["Quali informazioni aggiuntive mi servono per installare la mia attrezzatura che non è presente in HWU?"](#)[^] per maggiori informazioni sui requisiti di installazione dello switch.

Requisiti di configurazione

Per configurare un cluster, è necessario disporre del numero e del tipo appropriati di cavi e connettori per gli switch del cluster. A seconda del tipo di switch cluster che si sta configurando inizialmente, è necessario connettersi alla porta della console dello switch tramite il cavo della console incluso.

Assegnazioni delle porte dello switch del cluster

È possibile utilizzare la tabella delle assegnazioni delle porte dello switch del cluster BES-53248 supportata da Broadcom come guida per la configurazione del cluster.

Porte di commutazione	Utilizzo delle porte
01-16	Nodi porta cluster 10/25GbE, configurazione di base
17-48	Nodi di porta cluster 10/25GbE, con licenze
49-54	Nodi porta cluster 40/100GbE, con licenze, aggiunti da destra a sinistra
55-56	Porte Inter-Switch Link (ISL) del cluster 100GbE, configurazione di base

Vedi il ["Hardware Universe"](#) per maggiori informazioni sulle porte dello switch. 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.

Vincolo di velocità del gruppo di porte

- Negli switch cluster BES-53248, le 48 porte 10/25GbE (SFP28/SFP+) sono combinate in 12 gruppi da 4 porte come segue: Porte 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 e 45-48.
- La velocità della porta SFP28/SFP+ deve essere la stessa (10 GbE o 25 GbE) su tutte le porte del gruppo a 4 porte.

Requisiti aggiuntivi

- Se acquisti licenze aggiuntive, vedi ["Attiva le nuove porte di licenza"](#) per i dettagli su come attivarli.
- Se SSH è attivo, è necessario riattivarlo manualmente dopo aver eseguito il comando `erase startup-config` e riavviare lo switch.

Cosa c'è dopo?

Dopo aver esaminato i requisiti di configurazione, puoi confermare il tuo ["componenti e numeri di parte"](#).

Componenti e numeri di parte per gli switch cluster BES-53248

Per l'installazione e la manutenzione dell'interruttore BES-53248, assicurarsi di rivedere l'elenco dei componenti e i codici articolo.

Nella tabella seguente sono elencati il codice articolo, la descrizione e le versioni minime EFOS e ONTAP per i componenti dello switch cluster BES-53248, inclusi i dettagli del kit di guide per montaggio su rack.



Per i codici articolo **X190005-B** e **X190005R-B** è richiesta una versione EFOS minima **3.10.0.3**.

Numero di parte	Descrizione	Versione minima EFOS	Versione minima ONTAP
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = scarico lato sinistro)	3.10.0.3	9,8
X190005R-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PSIN (PSIN = ingresso lato porta)	3.10.0.3	9,8
X190005	BES-53248, CLSW, 16Pt10/25GB, PTSX, BRDCM SUPP	3.4.4.6	9.5P8
X190005R	BES-53248, CLSW, 16Pt10/25GB, PSIN, BRDCM SUPP	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Kit di montaggio su rack Ozeki 4 montanti 19"	N / A	N / A



Per quanto riguarda i tipi di macchina, tenere presente le seguenti informazioni:

Tipo di macchina	Versione minima EFOS
BES-53248A1	3.4.4.6
BES-53248A2	3.10.0.3
BES-53248A3	3.10.0.3

Puoi determinare il tipo specifico della tua macchina utilizzando il comando: `show version`

Mostra esempio

```
(cs1)# show version
```

```
Switch: cs1
```

```
System Description..... EFOS, 3.10.0.3, Linux  
5.4.2-b4581018, 2016.05.00.07  
Machine Type..... BES-53248A3  
Machine Model..... BES-53248  
Serial Number..... QTCU225xxxxx  
Part Number..... 1IX8BZxxxxx  
Maintenance Level..... a3a  
Manufacturer..... QTMC  
Burned In MAC Address..... C0:18:50:F4:3x:xx  
Software Version..... 3.10.0.3  
Operating System..... Linux 5.4.2-b4581018  
Network Processing Device..... BCM56873_A0  
.  
.  
.
```

Cosa c'è dopo?

Dopo aver confermato i componenti e i numeri di parte, puoi rivedere il ["documentazione richiesta"](#).

Requisiti di documentazione per gli switch cluster BES-53248

Per l'installazione e la manutenzione dello switch BES-53248, assicurarsi di consultare la documentazione specifica dello switch e del controller.

Documentazione Broadcom

Per configurare lo switch cluster BES-53248, sono necessari i seguenti documenti, disponibili sul sito di supporto Broadcom: ["Linea di prodotti Broadcom Ethernet Switch"](#)

Titolo del documento	Descrizione
<i>Guida dell'amministratore di EFOS v3.4.3</i>	Fornisce esempi di come utilizzare lo switch BES-53248 in una rete tipica.
<i>Riferimento ai comandi CLI EFOS v3.4.3</i>	Descrive i comandi dell'interfaccia della riga di comando (CLI) utilizzati per visualizzare e configurare il software BES-53248.
<i>Guida introduttiva a EFOS v3.4.3</i>	Fornisce informazioni dettagliate sullo switch BES-53248.

Titolo del documento	Descrizione
<i>Guida di riferimento SNMP EFOS v3.4.3</i>	Fornisce esempi di come utilizzare lo switch BES-53248 in una rete tipica.
<i>Parametri e valori di ridimensionamento EFOS v3.4.3</i>	Descrive i parametri di ridimensionamento predefiniti con cui il software EFOS viene distribuito e convalidato sulle piattaforme supportate.
<i>Specifiche funzionali EFOS v3.4.3</i>	Descrive le specifiche del software EFOS sulle piattaforme supportate.
Note sulla versione EFOS v3.4.3	Fornisce informazioni specifiche sulla versione del software BES-53248.
<i>Matrice di compatibilità della rete di cluster e della rete di gestione</i>	Fornisce informazioni sulla compatibilità di rete. La matrice è disponibile sul sito di download dello switch BES-53248 all'indirizzo "Switch cluster Broadcom" .

Documentazione dei sistemi ONTAP e articoli della Knowledge Base

Per configurare un sistema ONTAP , sono necessari i seguenti documenti dal sito di supporto NetApp all'indirizzo ["mysupport.netapp.com"](https://mysupport.netapp.com) o il sito della Knowledgebase (KB) all'indirizzo ["kb.netapp.com"](https://kb.netapp.com) .

Nome	Descrizione
"Hardware Universe NetApp"	Descrive i requisiti di alimentazione e di sito per tutto l'hardware NetApp , compresi gli armadi di sistema, e fornisce informazioni sui connettori e sulle opzioni di cavi pertinenti da utilizzare, insieme ai relativi codici articolo.
Istruzioni di installazione e configurazione specifiche del controller	Descrive come installare l'hardware NetApp .
ONTAP 9	Fornisce informazioni dettagliate su tutti gli aspetti della versione ONTAP 9.
<i>Come aggiungere licenze di porta aggiuntive per lo switch BES-53248 supportato da Broadcom</i>	Fornisce informazioni dettagliate sull'aggiunta di licenze di porta. Vai al "Articolo della Knowledge Base" .

Installare l'hardware

Flusso di lavoro di installazione hardware per gli switch BES-53248

Per installare e configurare l'hardware per uno switch cluster BES-53248, attenersi alla seguente procedura:



"Installare l'hardware dello switch"

Installare e configurare l'hardware dello switch BES-53248.

2

"Rivedere il cablaggio e la configurazione"

Esaminare le considerazioni sul cablaggio e sulla configurazione per lo switch cluster BES-53248.

Installare l'hardware per lo switch cluster BES-53248

Per installare l'hardware BES-53248, fare riferimento alla documentazione Broadcom.

Passi

1. Rivedere il ["requisiti di configurazione"](#) .
2. Seguire le istruzioni nel ["Guida all'installazione dello switch cluster BES-53248 supportato da Broadcom"](#) .

Cosa succederà ora?

Dopo aver installato l'hardware per lo switch, puoi ["rivedere il cablaggio e la configurazione"](#) requisiti.

Esaminare le considerazioni sul cablaggio e sulla configurazione

Prima di configurare lo switch Broadcom BES-53248, leggere le seguenti considerazioni.

Assegnazioni degli switch delle porte del cluster

È possibile utilizzare la tabella delle assegnazioni delle porte dello switch del cluster BES-53248 supportata da Broadcom come guida per configurare il cluster.

Porte di commutazione	Utilizzo delle porte
0-16	Nodi porta cluster 10/25GbE, configurazione di base
17-48	Nodi di porta cluster 10/25GbE, con licenze
49-54	Nodi porta cluster 40/100GbE, con licenze, aggiunti da destra a sinistra
55-56	Porte Inter-Switch Link (ISL) del cluster 100GbE, configurazione di base

Vedi il ["Hardware Universe"](#) per maggiori informazioni sulle porte dello switch. 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.

Vincolo di velocità del gruppo di porte

- Negli switch cluster BES-53248, le 48 porte 10/25GbE (SFP28/SFP+) sono combinate in 12 gruppi da 4 porte come segue: Porte 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 e 45-48.
- La velocità della porta SFP28/SFP+ deve essere la stessa (10 GbE o 25 GbE) su tutte le porte del gruppo a 4 porte.
- Se le velocità in un gruppo a 4 porte sono diverse, le porte dello switch non funzioneranno correttamente.

Requisiti FEC

- Per i dettagli sulle porte 25G con cavi in rame, vedere la tabella seguente.

Se il lato Controller è `auto` , il lato dell'interruttore è impostato su FEC 25G.

FAS2820 FEC			Switch FEC			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	UP
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP

- Per le porte 25G con cavi in fibra/ottica, vedere la seguente tabella per i dettagli:

FAS2820 FEC			Switch FEC			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	DOWN
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN

Implementazione di Bootarg

Utilizzare il seguente comando per impostare la porta 25G FEC su `auto` O `fc` , come richiesto:

```
systemshell -node <node> -command sudo sysctl  
dev.ice.<X>.requested_fec=<auto/fc>
```

- Quando impostato su `*auto *`:
 - IL `auto` l'impostazione propaga immediatamente l'impostazione all'hardware e non è necessario alcun riavvio.
 - Se `bootarg.cpk_fec_fc_eXx already exists`, viene eliminato dalla memoria `bootarg`.
 - Dopo un riavvio, il `auto` l'impostazione rimane in vigore da quando `auto` è l'impostazione FEC predefinita.
- Quando impostato su `*fc *`:
 - IL `FC-FEC` l'impostazione propaga immediatamente l'impostazione all'hardware e non è necessario alcun riavvio.
 - Un nuovo `bootarg.cpk_fec_fc_eXx` viene creato con il valore impostato su `"true"`.
 - Dopo un riavvio, `FC-FEC` l'impostazione rimane attiva affinché il codice del driver possa utilizzarla.

Configurare il software

Flusso di lavoro di installazione del software per gli switch BES-53248

Per installare e configurare il software per uno switch cluster BES-53248, attenersi alla seguente procedura:

1

"Configurare l'interruttore"

Configurare lo switch cluster BES-53248.

2

"Installa il software EFOS"

Scaricare e installare il software Ethernet Fabric OS (EFOS) sullo switch cluster BES-53248.

3

"Installa le licenze per gli switch cluster BES-53248"

Facoltativamente, puoi aggiungere nuove porte acquistando e installando più licenze. Il modello base dello switch è concesso in licenza per 16 porte 10GbE o 25GbE e due porte 100GbE.

4

"Installare il file di configurazione di riferimento (RCF)"

Installare o aggiornare l'RCF sullo switch cluster BES-53248, quindi verificare le porte per una licenza aggiuntiva dopo l'applicazione dell'RCF.

5

"Abilita SSH sugli switch cluster BES-53248"

Se si utilizzano le funzionalità di monitoraggio dello stato dello switch Ethernet (CSHM) e di raccolta dei

registri, abilitare SSH sugli switch.



"Ripristinare l'interruttore alle impostazioni predefinite di fabbrica"

Cancellare le impostazioni dello switch del cluster BES-53248.

Configurare lo switch cluster BES-53248

Per eseguire la configurazione iniziale dello switch cluster BES-53248, attenersi alla seguente procedura.

Prima di iniziare

- L'hardware è installato, come descritto in ["Installare l'hardware"](#).
- Hai esaminato quanto segue:
 - ["Requisiti di configurazione"](#)
 - ["Componenti e numeri di parte"](#)
 - ["Requisiti di documentazione"](#)

Informazioni sugli esempi

Gli esempi nelle procedure di configurazione utilizzano la seguente nomenclatura di switch e nodi:

- I nomi degli switch NetApp sono `cs1` e `cs2`. L'aggiornamento inizia sul secondo switch, `cs2`.
- I nomi LIF del cluster sono `node1_clus1` e `node1_clus2` per il nodo 1 e `node2_clus1` e `node2_clus2` per il nodo 2.
- Il nome dello spazio IP è Cluster.
- IL `cluster1 :>` il prompt indica il nome del cluster.
- Le porte del cluster su ciascun nodo sono denominate `e0a` e `e0b`. Vedi il ["Hardware Universe NetApp"](#) per le porte cluster effettivamente supportate sulla tua piattaforma.
- I collegamenti Inter-Switch (ISL) supportati per gli switch NetApp sono le porte 0/55 e 0/56.
- Le connessioni dei nodi supportate per gli switch NetApp sono le porte da 0/1 a 0/16 con licenza predefinita.
- Negli esempi vengono utilizzati due nodi, ma è possibile avere fino a 24 nodi in un cluster.

Passi

1. Collegare la porta seriale a un host o a una porta seriale.
2. Collegare la porta di gestione (la porta RJ-45 sul lato sinistro dello switch) alla stessa rete in cui si trova il server TFTP.
3. Nella console, impostare le impostazioni seriali lato host:
 - 115200 baud
 - 8 bit di dati
 - 1 bit di stop
 - parità: nessuna
 - controllo di flusso: nessuno

4. Accedi allo switch come `admin` e premere **Invio** quando viene richiesta una password. Il nome predefinito dello switch è **routing**. Al prompt, immettere `enable` . Ciò consente di accedere alla modalità Privileged EXEC per la configurazione dello switch.

```
User: admin
Password:
(Routing)> enable
Password:
(Routing) #
```

5. Cambia il nome dello switch in **cs2**.

```
(Routing) # hostname cs2
(cs2) #
```

6. Per impostare un indirizzo di gestione IPv4 o IPv6 statico per la porta di servizio dello switch:

IPv4

Per impostazione predefinita, la porta di servizio è impostata per utilizzare DHCP. L'indirizzo IP, la maschera di sottorete e l'indirizzo del gateway predefinito vengono assegnati automaticamente.

```
(cs2) # serviceport protocol none
(cs2) # network protocol none
(cs2) # serviceport ip <ip-address> <netmask> <gateway>
```

IPv6

Per impostazione predefinita, la porta di servizio è impostata per utilizzare DHCP. L'indirizzo IP, la maschera di sottorete e l'indirizzo del gateway predefinito vengono assegnati automaticamente.

```
(cs2) # serviceport protocol none
(cs2) # network protocol none
(cs2) # serviceport ipv6 <address>
(cs2) # serviceport ipv6 <gateway>
```

1. Verificare i risultati utilizzando il comando:

```
show serviceport
```

```
(cs2)# show serviceport
Interface Status..... Up
IP Address..... 172.19.2.2
Subnet Mask..... 255.255.255.0
Default Gateway..... 172.19.2.254
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::dac4:97ff:fe71:123c/64
IPv6 Default Router..... fe80::20b:45ff:fea9:5dc0
Configured IPv4 Protocol..... DHCP
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Burned In MAC Address..... D8:C4:97:71:12:3C
```

2. Configurare il dominio e il name server:

```
ip domain name <domain_name>
ip name server <server_name>
```

```
(cs2)# configure
(cs2) (Config)# ip domain name company.com
(cs2) (Config)# ip name server 10.10.99.1 10.10.99.2
(cs2) (Config)# exit
(cs2)#
```

3. Configurare il server NTP.

EFOS 3.10.0.3 e versioni successive

Configurare il fuso orario e la sincronizzazione dell'ora (NTP):

```
sntp server <server_name>  
clock
```

```
(cs2)# configure  
(cs2)(Config)# ntp server 10.99.99.5  
(cs2)(Config)# clock timezone -7  
(cs2)(Config)# exit  
(cs2)#
```

EFOS 3.9.0.2 e precedenti

Configurare il fuso orario e la sincronizzazione dell'ora (SNTP):

```
sntp client mode <client_mode>  
sntp server <server_name>  
clock
```

```
(cs2)# configure  
(cs2)(Config)# sntp client mode unicast  
(cs2)(Config)# sntp server 10.99.99.5  
(cs2)(Config)# clock timezone -7  
(cs2)(Config)# exit  
(cs2)#
```

1. Configurare l'ora manualmente se non è stato configurato un server NTP nel passaggio precedente.

EFOS 3.10.0.3 e versioni successive

Configurare l'ora manualmente.

clock

```
(cs2)# configure
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 e precedenti

Configurare l'ora manualmente.

clock

```
(cs2)# configure
(cs2)(Config)# no sntp client mode
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

1. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
write memory
```

```
(cs2)# write memory
```

```
This operation may take a few minutes.
```

```
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

Cosa succederà ora?

Dopo aver configurato gli switch, puoi ["installare il software EFOS"](#).

Installa il software EFOS

Per installare il software Ethernet Fabric OS (EFOS) sullo switch cluster BES-53248, seguire questi passaggi.

Il software EFOS include una serie di funzionalità e protocolli di rete avanzati per lo sviluppo di sistemi infrastrutturali Ethernet e IP. Questa architettura software è adatta a qualsiasi dispositivo organizzativo di rete che utilizzi applicazioni che richiedono un'ispezione o una separazione completa dei pacchetti.

Prepararsi per l'installazione

Prima di iniziare

- Questa procedura è adatta solo per le nuove installazioni.
- Scarica il software Broadcom EFOS applicabile per i tuoi switch cluster da ["Supporto per switch Ethernet Broadcom"](#) sito.
- Assicurare il ["Lo switch cluster BES-53248 è configurato"](#) .

Installa il software

Per installare il software EFOS, utilizzare uno dei seguenti metodi:

- [Metodo 1: installare EFOS](#). Da utilizzare nella maggior parte dei casi.
- [Metodo 2: installare EFOS in modalità ONIE](#). Utilizzare se una versione di EFOS è conforme a FIPS e l'altra non lo è.

Metodo 1: installare EFOS

Per installare il software EFOS, procedere come segue.

Passi

1. Accedere alla porta della console seriale dello switch o connettersi tramite SSH.
2. Utilizzare il `ping` comando per verificare la connettività al server che ospita EFOS, le licenze e il file RCF.

Mostra esempio

Questo esempio verifica che lo switch sia connesso al server all'indirizzo IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

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

3. Scarica il file immagine sullo switch.

Per informazioni sui protocolli di copia supportati, consultare la seguente tabella:

Protocollo	Prerequisito
Protocollo di trasferimento file banale (TFTP)	Nessuno
Protocollo di trasferimento file SSH (SFTP)	Il tuo pacchetto software deve supportare la gestione sicura
FTP	Password richiesta
XMODEM	Nessuno
YMODEM	Nessuno
ZMODEM	Nessuno
Protocollo di copia sicura (SCP)	Il tuo pacchetto software deve supportare la gestione sicura
HTTP	Trasferimenti di file basati su CLI supportati su piattaforme selezionate quando è disponibile un'utilità WGET nativa
HTTPS	Trasferimenti di file basati su CLI supportati su piattaforme selezionate quando è disponibile un'utilità WGET nativa

Copiando il file immagine nell'immagine attiva, al riavvio tale immagine stabilisce la versione EFOS in esecuzione. L'immagine precedente rimane disponibile come backup.

Mostra esempio

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk active
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.10.0.3.stk
Data Type..... Code
Destination Filename..... active

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...

File transfer operation completed successfully.
```

4. Visualizza le immagini di avvio per la configurazione attiva e di backup:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1         3.7.0.4      3.7.0.4      3.7.0.4              3.10.0.3
```

5. Riavviare lo switch:

```
reload
```

Mostra esempio

```
(cs2)# reload
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully .
```

```
Configuration Saved!
```

```
System will now restart!
```

6. Effettua nuovamente l'accesso e verifica la nuova versione del software EFOS:

```
show version
```

Mostra esempio

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04  
Machine Type..... BES-53248A1,  
Machine Model..... BES-53248  
Serial Number..... QTFCU38260023  
Maintenance Level..... A  
Manufacturer..... 0xbc00  
Burned In MAC Address..... D8:C4:97:71:0F:40  
Software Version..... 3.10.0.3  
Operating System..... Linux 4.4.211-  
28a6fe76  
Network Processing Device..... BCM56873_A0  
CPLD Version..... 0xff040c03
```

```
Additional Packages..... BGP-4  
..... QOS  
..... Multicast  
..... IPv6  
..... Routing  
..... Data Center  
..... OpEN API  
..... Prototype Open API
```

7. Completare l'installazione. Per riconfigurare lo switch, seguire questi quattro passaggi:
 - a. "Installa le licenze"
 - b. "Installa il file RCF"
 - c. "Abilita SSH"
 - d. "Configurare il monitoraggio dello stato dello switch"
8. Ripetere i passaggi da 1 a 7 sul cambio partner.

Metodo 2: installare EFOS in modalità ONIE

È possibile eseguire i seguenti passaggi se una versione di EFOS è conforme a FIPS e l'altra non lo è. Questi passaggi possono essere utilizzati per installare l'immagine EFOS 3.7.xx non FIPS o conforme a FIPS da ONIE se lo switch non riesce ad avviarsi.

Passi

1. Connettersi a una console collegata alla porta seriale dello switch.
2. Avviare lo switch in modalità di installazione ONIE.

Durante l'avvio, selezionare ONIE quando viene visualizzato il prompt.

Mostra esempio

Diagram illustrating a vertical stack of 20 horizontal bars. The top bar is labeled 'EFOS' and the second bar is labeled '*ONIE'. The bars are arranged in a column, with dashed lines at the top and bottom.

Dopo aver selezionato **ONIE**, l'interruttore si carica e ti presenta diverse scelte. Selezionare **Installa sistema operativo**.

Mostra esempio

```

+-----+
-+
|*ONIE:  Install OS
|
|  ONIE:  Rescue
|
|  ONIE:  Uninstall OS
|
|  ONIE:  Update ONIE
|
|  ONIE:  Embed ONIE
|
|  DIAG:  Diagnostic Mode
|
|  DIAG:  Burn-In Mode
|
|
|
|
|
|
|
|
|
|
+-----+
-+

```

Lo switch si avvia in modalità di installazione ONIE.

3. Interrompere la scoperta ONIE e configurare l'interfaccia Ethernet.

Quando viene visualizzato il seguente messaggio, premere **Invio** per richiamare la console ONIE:

```
Please press Enter to activate this console. Info: eth0:  Checking
link... up.
ONIE:/ #
```



La scoperta ONIE continua e i messaggi vengono stampati sulla console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

4. Configurare l'interfaccia Ethernet della porta di gestione dello switch e aggiungere il percorso utilizzando
`ifconfig eth0 <ipAddress> netmask <netmask> up` `E route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

5. Verificare che il server che ospita il file di installazione ONIE sia raggiungibile:

ping

Mostra esempio

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

6. Installa il nuovo software dello switch:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

Mostra esempio

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Il software installa e poi riavvia lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione EFOS.

7. Accedi e verifica che il nuovo software dello switch sia installato:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
-----
unit    active      backup    current-active  next-active
-----
  1      3.7.0.4        3.7.0.4        3.7.0.4         3.10.0.3
(cs2) #
```

8. Completare l'installazione. Lo switch si riavvia senza alcuna configurazione applicata e ripristina le impostazioni predefinite di fabbrica. Per riconfigurare lo switch, seguire questi cinque passaggi:
- ["Configurare l'interruttore"](#)
 - ["Installa le licenze"](#)
 - ["Installa il file RCF"](#)
 - ["Abilita SSH"](#)

e. ["Configurare il monitoraggio dello stato dello switch"](#)

9. Ripetere i passaggi da 1 a 8 sullo switch partner.

Cosa c'è dopo?

Dopo aver installato il software EFOS, puoi ["installa le tue licenze"](#).

Installare il file di configurazione di riferimento (RCF) e il file di licenza

A partire da EFOS 3.12.0.1, è possibile installare il file di configurazione di riferimento (RCF) e il file di licenza dopo aver configurato lo switch cluster BES-53248.



Tutte le porte sono configurate quando si installa RCF, ma è necessario installare la licenza per attivare le porte configurate.

Requisiti di revisione

Prima di iniziare

Verificare che quanto segue sia presente:

- Un backup attuale della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- L'attuale RCF, disponibile presso ["Switch cluster Broadcom"](#) pagina.
- Una configurazione di avvio nell'RCF che riflette le immagini di avvio desiderate, necessaria se si installa solo EFOS e si mantiene la versione RCF corrente. 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.
- Una connessione della console allo switch, necessaria quando si installa l'RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.

Documentazione suggerita

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedi il ["Scarica il software EFOS"](#) pagina. Si noti che possono esserci dipendenze tra la sintassi dei comandi nella RCF e quella presente nelle versioni di EFOS.

Installa il file di configurazione

Informazioni sugli esempi

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

- I nomi dei due switch BES-53248 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.

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi dello switch Broadcom; 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 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, utilizzare l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#). Se è necessario cancellare completamente le impostazioni dello switch, è necessario eseguire nuovamente la configurazione di base. È necessario connettersi allo switch tramite la console seriale perché una cancellazione completa della configurazione reimposta la configurazione della rete di gestione.

Fase 1: Preparazione all'installazione

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.

Il seguente comando sopprime la creazione automatica dei casi per due ore:

```
cluster1::*> system node autosupport invoke -node \* -type all -message MAINT=2h
```

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

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                0/2          BES-
53248
          e0b    cs2                0/2          BES-
53248
cluster1-02/cdp
          e0a    cs1                0/1          BES-
53248
          e0b    cs2                0/1          BES-
53248
cluster1-03/cdp
          e0a    cs1                0/4          BES-
53248
          e0b    cs2                0/4          BES-
53248
cluster1-04/cdp
          e0a    cs1                0/3          BES-
53248
          e0b    cs2                0/3          BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```
Ignore
```

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

b. 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	
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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                               Type                Address             Model
-----
cs1                                  cluster-network     10.228.143.200     BES-
53248
    Serial Number: QTWCU22510008
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP

cs2                                  cluster-network     10.228.143.202     BES-
53248
    Serial Number: QTWCU22510009
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Disabilitare il ripristino automatico sui LIF del cluster.

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

Passaggio 2: configurare le porte

1. Sullo switch cs2, confermare l'elenco delle porte connesse ai nodi nel cluster.

```
show isdp neighbor
```

2. Sullo switch del cluster cs2, chiudere le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono collegate ai nodi ONTAP :

```
(cs2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)#
```

3. Verificare che i LIF del cluster siano stati migrati alle 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::*>				

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
```

5. Se non lo hai già fatto, salva la configurazione corrente dello switch copiando l'output del seguente comando in un file di registro:

```
show running-config
```

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



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Per cancellare le impostazioni dello switch è necessario essere connessi allo switch tramite la console seriale. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.



La cancellazione della configurazione non elimina le licenze.

- a. Accedi allo switch tramite SSH.

Procedere solo quando tutti i cluster LIF sono stati rimossi dalle porte sullo switch e lo switch è pronto per la cancellazione della configurazione.

- b. Entra in modalità privilegio:

```
(cs2)> enable
(cs2)#
```

- c. Copia e incolla i seguenti comandi per rimuovere la precedente configurazione RCF (a seconda della precedente versione RCF utilizzata, alcuni comandi potrebbero generare un errore se una particolare impostazione non è presente):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```

```

configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDst
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit

```

d. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
(cs2)# write memory
```

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) **y**

Config file 'startup-config' created successfully.

Configuration Saved!

e. Eseguire un riavvio dello switch:

```
(cs2)# reload
```

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

f. Accedere nuovamente allo switch tramite SSH per completare l'installazione RCF.

7. Registrare tutte le personalizzazioni apportate nel precedente RCF e applicarle al nuovo RCF. Ad esempio, impostando la velocità delle porte o codificando la modalità FEC.
8. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: FTP, HTTP, TFTP, SFTP o SCP.

Questo esempio mostra l'utilizzo di HTTP per copiare un RCF nel bootflash sullo switch cs2:

Mostra esempio

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-RCF-v1.12-Cluster-HA.txt nvram:reference-config

Mode..... HTTP
Set Server IP..... 172.19.2.1
Path..... <ip-to-
webserver>/path/to/
Filename..... BES-53248-RCF-v1.12-Cluster-HA.txt
Data Type..... Unknown

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
File transfer in progress.
Management access will be blocked for the duration of the transfer.
Please wait...
HTTP Unknown file type transfer starting...
Validating configuration script.....
Configuration script validated.
File transfer operation completed successfully.
```

9. Verifica che lo script sia stato scaricato e salvato con il nome file che gli hai assegnato:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
Reference-config.scr 21:54:22	2680	2024 05 31

```
1 configuration script(s) found.
2045 Kbytes free.
```

10. Applica lo script allo switch:

```
script apply
```

Mostra esempio

```
(cs2)# script apply reference-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!
...
...
Configuration script 'reference-config.scr' applied.
```

11. Installare il file di licenza.

Mostra esempio

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-LIC.dat
nvram:license-key 1
Mode..... HTTP
Set Server IP..... 172.19.2.1
Path..... <ip-to-
webserver>/path/to/
Filename..... BES-53248-LIC.dat
Data Type..... license

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer.

Please wait...

License Key transfer operation completed successfully.

System reboot is required.
(cs2)# write memory

This operation may take a few minutes.

Management interfaces will not be available during this time.
Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!

(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
...
...
```

12. Esaminare l'output del banner dal `show clibanner` comando. È necessario leggere e seguire queste istruzioni per verificare la corretta configurazione e il corretto funzionamento dello switch.

Mostra esempio

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.12 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename  : BES-53248-RCF-v1.12-Cluster.txt
```

```
Date      : 11-04-2024
```

```
Version   : v1.12
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms of port speed:

- Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44, 45-48

- The port speed should be the same (10GbE or 25GbE) across all ports in a 4-port group

- If additional licenses are purchased, follow the 'Additional Node Ports

- activated with Licenses' section for instructions

- If SSH is active, it will have to be re-enabled manually after 'erase startup-config'

- command has been executed and the switch rebooted"

13. Sullo switch, verificare che le porte con licenza aggiuntive vengano visualizzate dopo l'applicazione dell'RCF:

```
show port all | exclude Detach
```

Mostra esempio

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

14. Sullo switch, verifica che le modifiche siano state apportate:

```
show running-config
```

```
(cs2)# show running-config
```

15. Salvare la configurazione in esecuzione in modo che diventi la configurazione di avvio quando si riavvia lo switch:

```
write memory
```

```
(cs2)# write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

16. Riavviare lo switch e verificare che la configurazione in esecuzione sia corretta:

```
reload
```

```
(cs2)# reload
```

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

```
System will now restart!
```

17. Sullo switch del cluster cs2, richiamare le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono collegate ai nodi ONTAP :

```
(cs2)> enable
```

```
(cs2)# configure
```

```
(cs2) (Config)# interface 0/1-0/16
```

```
(cs2) (Interface 0/1-0/16)# no shutdown
```

```
(cs2) (Interface 0/1-0/16)# exit
```

```
(cs2) (Config)#
```

18. Verificare le porte sullo switch cs2:

```
show interfaces status all | exclude Detach
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Verificare che le porte e0b 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					
e0b	Cluster	Cluster		up	9000	auto/100000
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/100000
healthy	false					
e0b	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	0/2
BES-53248			
	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp			
	e0a	cs1	0/1
BES-53248			
	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp			
	e0a	cs1	0/4
BES-53248			
	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp			
	e0a	cs1	0/3
BES-53248			
	e0b	cs2	0/2
BES-53248			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

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

L'esempio seguente utilizza l'output dell'esempio di interfaccia:

```
(cs1)> enable
(cs1)# configure
(cs1) (Config)# interface 0/1-0/16
(cs1) (Interface 0/1-0/16)# shutdown
```

2. 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	e0a	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	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	e0a	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
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. Ripetere i passaggi da 4 a 19 sullo switch cs1.

5. Abilita il ripristino automatico sui LIF del cluster:

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

6. Riavviare lo switch cs1. Ciò fa sì che i LIF del cluster tornino alle loro porte di origine. È possibile ignorare gli eventi "porte cluster inattive" segnalati sui nodi durante il riavvio dello switch.

```
(cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved! System will now restart!
```

Passaggio 3: verificare la configurazione

1. Sullo switch cs1, verificare che le porte dello switch connesse alle porte del cluster siano **attive**:

```
show interfaces status all | exclude Detach
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Verificare che l'ISL tra gli switch cs1 e cs2 sia funzionante:

```
show port-channel 1/1
```

Mostra esempio

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----  -
0/55     actor/long      Auto      True
         partner/long
0/56     actor/long      Auto      True
         partner/long
```

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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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 `show` comando per visualizzare i dettagli.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
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)

```

1. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver installato il file RCF e la licenza, puoi ["abilita SSH"](#).

Installa le licenze per gli switch cluster BES-53248

Il modello base dello switch cluster BES-53248 è concesso in licenza per 16 porte 10GbE o 25GbE e due porte 100GbE. È possibile aggiungere nuove porte acquistando più licenze.



Per EFOS 3.12 e versioni successive, seguire i passaggi di installazione in ["Installare il file di configurazione di riferimento \(RCF\) e il file di licenza"](#).

Esamina le licenze disponibili

Le seguenti licenze sono disponibili per l'uso sullo switch cluster BES-53248:

Tipo di licenza	Dettagli della licenza	Versione firmware supportata
SW-BES-53248A2-8P-2P	Chiave di licenza Broadcom 8PT-10G25G + 2PT-40G100G, X190005/R	EFOS 3.4.4.6 e versioni successive
SW-BES-53248A2-8P-1025G	Chiave di licenza Broadcom 8 porte 10G25G, X190005/R	EFOS 3.4.4.6 e versioni successive
SW-BES53248A2-6P-40-100G	Chiave di licenza Broadcom 6 porte 40G100G, X190005/R	EFOS 3.4.4.6 e versioni successive



Per riscattare una chiave di transazione per un file di chiave di licenza della porta, vai a ["Portale delle licenze per gli switch Ethernet supportati da Broadcom"](#) pagina. Vedi l'articolo della Knowledge Base ["Come aggiungere licenze di porta aggiuntive per lo switch Broadcom BES-53248"](#) per ulteriori dettagli.

Licenze legacy

Nella tabella seguente sono elencate le licenze legacy disponibili per l'uso sullo switch cluster BES-53248:

Tipo di licenza	Dettagli della licenza	Versione firmware supportata
SW-BES-53248A1-G1-8P-LIC	Chiave di licenza Broadcom 8P 10-25,2P40-100, X190005/R	EFOS 3.4.3.3 e versioni successive

Tipo di licenza	Dettagli della licenza	Versione firmware supportata
SW-BES-53248A1-G1-16P-LIC	Chiave di licenza Broadcom 16P 10-25,4P40-100, X190005/R	EFOS 3.4.3.3 e versioni successive
SW-BES-53248A1-G1-24P-LIC	Chiave di licenza Broadcom 24P 10-25,6P40-100, X190005/R	EFOS 3.4.3.3 e versioni successive
SW-BES54248-40-100G-LIC	Chiave di licenza Broadcom 6Port 40G100G, X190005/R	EFOS 3.4.4.6 e versioni successive
SW-BES53248-8P-10G25G-LIC	Chiave di licenza Broadcom 8Port 10G25G, X190005/R	EFOS 3.4.4.6 e versioni successive
SW-BES53248-16P-1025G-LIC	Chiave di licenza Broadcom 16Port 10G25G, X190005/R	EFOS 3.4.4.6 e versioni successive
SW-BES53248-24P-1025G-LIC	Chiave di licenza Broadcom 24Port 10G25G, X190005/R	EFOS 3.4.4.6 e versioni successive



Per la configurazione di base non è richiesta alcuna licenza.

Installa i file di licenza

Per installare le licenze per gli switch cluster BES-53248, seguire questi passaggi.

Passi

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il ping comando per verificare la connettività al server che ospita EFOS, le licenze e il file RCF.

Mostra esempio

Questo esempio verifica che lo switch sia connesso al server all'indirizzo IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

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

3. Controllare l'utilizzo attuale della licenza su switch cs2:

```
show license
```

Mostra esempio

```
(cs2)# show license
Reboot needed..... No
Number of active licenses..... 0

License Index  License Type      Status
-----
-----

No license file found.
```

4. Installare il file di licenza.

Ripetere questo passaggio per caricare altre licenze e utilizzare numeri di indice chiave diversi.

Mostra esempio

Nell'esempio seguente viene utilizzato SFTP per copiare un file di licenza in un indice chiave 1.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... /var/lib/tftpboot/
Filename..... license.dat
Data Type..... license

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...

License Key transfer operation completed successfully. System reboot
is required.
```

5. Visualizza tutte le informazioni sulla licenza corrente e prendi nota dello stato della licenza prima di riavviare lo switch cs2:

```
show license
```

Mostra esempio

```
(cs2)# show license
```

```
Reboot needed..... Yes
Number of active licenses..... 0
```

License Index	License Type	Status
1	Port	License valid but not applied

6. Visualizza tutte le porte con licenza:

```
show port all | exclude Detach
```

Le porte dei file di licenza aggiuntivi non vengono visualizzate finché lo switch non viene riavviato.

Mostra esempio



```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----	-----	-----	-----	-----	-----	-----	
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/55		Disable	Auto		Down	Enable	
Enable long							
0/56		Disable	Auto		Down	Enable	
Enable long							

7. Riavviare lo switch:

```
reload
```

Mostra esempio

```
(cs2)# reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully .

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

8. Verificare che la nuova licenza sia attiva e notare che la licenza è stata applicata:

```
show license
```

Mostra esempio

```
(cs2)# show license

Reboot needed..... No
Number of installed licenses..... 1
Total Downlink Ports enabled..... 16
Total Uplink Ports enabled..... 8

License Index  License Type                Status
-----
-----
1              Port                      License applied
```

9. Verificare che tutte le nuove porte siano disponibili:

```
show port all | exclude Detach
```

Mostra esempio

```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----		-----	-----	-----	-----	-----	
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/49		Disable	100G Full		Down	Enable	
Enable long							
0/50		Disable	100G Full		Down	Enable	
Enable long							

0/51	Disable	100G	Full	Down	Enable
Enable long					
0/52	Disable	100G	Full	Down	Enable
Enable long					
0/53	Disable	100G	Full	Down	Enable
Enable long					
0/54	Disable	100G	Full	Down	Enable
Enable long					
0/55	Disable	100G	Full	Down	Enable
Enable long					
0/56	Disable	100G	Full	Down	Enable
Enable long					



Quando si installano licenze aggiuntive, è necessario configurare manualmente le nuove interfacce. Non riapplicare un RCF a un interruttore di produzione funzionante esistente.

Risolvere i problemi di installazione

Se si verificano problemi durante l'installazione di una licenza, eseguire i seguenti comandi di debug prima di eseguire `copy` comando di nuovo.

Comandi di debug da utilizzare: `debug transfer` E `debug license`

Mostra esempio

```
(cs2)# debug transfer
Debug transfer output is enabled.
(cs2)# debug license
Enabled capability licensing debugging.
```

Quando esegui il `copy` comando con il `debug transfer` E `debug license` opzioni abilitate, viene restituito l'output del registro.

Mostra esempio

```
transfer.c(3083):Transfer process  key or certificate file type = 43
transfer.c(3229):Transfer process  key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
LICENSING :
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
    },
    "description": "",
    "ports": "0+6"
  }
}.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Model BES-53248
matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Applying license file
1.
```

Controllare quanto segue nell'output di debug:

- Verificare che il numero di serie corrisponda: Serial number QTFCU38290012 matched.
- Verificare che il modello dell'interruttore corrisponda: Model BES-53248 matched.
- Verificare che l'indice di licenza specificato non sia stato utilizzato in precedenza. Se è già utilizzato un indice di licenza, viene restituito il seguente errore: License file /mnt/download//license.dat.1 already exists.
- Una licenza di porta non è una licenza di funzionalità. Pertanto, ci si aspetta la seguente dichiarazione: Feature not found in license file with index = 1.

Utilizzare il copy comando per eseguire il backup delle licenze delle porte sul server:

```
(cs2) # copy nvram:license-key 1  
scp://<UserName>@<IP_address>/saved_license_1.dat
```



Se è necessario effettuare il downgrade del software dello switch dalla versione 3.4.4.6, le licenze vengono rimosse. Questo è un comportamento previsto.

Prima di tornare a una versione precedente del software, è necessario installare una licenza precedente appropriata.

Attiva le porte appena concesse in licenza

Per attivare le porte con licenza recente, è necessario modificare l'ultima versione dell'RCF e rimuovere il commento dai dettagli della porta applicabile.

La licenza predefinita attiva le porte da 0/1 a 0/16 e da 0/55 a 0/56, mentre le porte appena assegnate saranno comprese tra le porte da 0/17 a 0/54, a seconda del tipo e del numero di licenze disponibili. Ad esempio, per attivare la licenza SW-BES54248-40-100G-LIC, è necessario rimuovere il commento dalla seguente sezione nell'RCF:

Mostra esempio

```
.
.
!
! 2-port or 6-port 40/100GbE node port license block
!
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
.
.
```



Per le porte ad alta velocità comprese tra 0/49 e 0/54 incluse, rimuovere il commento da ciascuna porta, ma rimuovere il commento da una sola riga **speed** nell'RCF per ciascuna di queste porte, ovvero: **speed 100G full-duplex** o **speed 40G full-duplex** come mostrato nell'esempio. Per le porte a bassa velocità comprese tra 0/17 e 0/48 incluse, rimuovere il commento dall'intera sezione a 8 porte quando è stata attivata una licenza appropriata.

Cosa succederà ora?

Dopo aver installato le licenze, puoi ["installare il file di configurazione di riferimento \(RCF\)"](#) O ["aggiornare l'RCF"](#).

Installare il file di configurazione di riferimento (RCF)

È possibile installare il file di configurazione di riferimento (RCF) dopo aver configurato lo switch cluster BES-53248 e dopo aver applicato le nuove licenze.



Per EFOS 3.12 e versioni successive, seguire i passaggi di installazione in ["Installare il file di configurazione di riferimento \(RCF\) e il file di licenza"](#).

Requisiti di revisione

Prima di iniziare

Verificare che quanto segue sia presente:

- Un backup attuale della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Il file RCF corrente, disponibile da ["Switch cluster Broadcom"](#) pagina.
- Una configurazione di avvio nell'RCF che riflette le immagini di avvio desiderate, necessaria se si installa solo EFOS e si mantiene la versione RCF corrente. 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.
- Una connessione della console allo switch, necessaria quando si installa l'RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.

Documentazione suggerita

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedi il ["Scarica il software EFOS"](#) pagina. Si noti che possono esserci dipendenze tra la sintassi dei comandi nella RCF e quella presente nelle versioni di EFOS.

Installa il file di configurazione

Informazioni sugli esempi

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

- I nomi dei due switch BES-53248 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.

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi dello switch Broadcom; 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 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, utilizzare l'articolo della Knowledge Base "[Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota](#)". Se è necessario cancellare completamente le impostazioni dello switch, è necessario eseguire nuovamente la configurazione di base. È necessario connettersi allo switch tramite la console seriale perché una cancellazione completa della configurazione reimposta la configurazione della rete di gestione.

Fase 1: Preparazione all'installazione

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.

Il seguente comando sopprime la creazione automatica dei casi per due ore:

```
cluster1::*> system node autosupport invoke -node \* -type all -message  
MAINT=2h
```

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

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                      0/2          BES-
53248
           e0b    cs2                      0/2          BES-
53248
cluster1-02/cdp
           e0a    cs1                      0/1          BES-
53248
           e0b    cs2                      0/1          BES-
53248
cluster1-03/cdp
           e0a    cs1                      0/4          BES-
53248
           e0b    cs2                      0/4          BES-
53248
cluster1-04/cdp
           e0a    cs1                      0/3          BES-
53248
           e0b    cs2                      0/3          BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
cluster1::*>
```

b. 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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Disabilitare il ripristino automatico sui LIF del cluster.

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

Passaggio 2: configurare le porte

1. Sullo switch cs2, confermare l'elenco delle porte connesse ai nodi nel cluster.

```
show isdp neighbor
```

2. Sullo switch del cluster cs2, chiudere le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono collegate ai nodi ONTAP :

```
(cs2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)#
```

3. Verificare che i LIF del cluster siano stati migrati alle 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::*>				

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
```

5. Se non lo hai già fatto, salva la configurazione corrente dello switch copiando l'output del seguente comando in un file di registro:

```
show running-config
```

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



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Per cancellare le impostazioni dello switch è necessario essere connessi allo switch tramite la console seriale. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.



La cancellazione della configurazione non elimina le licenze.

- a. Accedi allo switch tramite SSH.

Procedere solo quando tutti i cluster LIF sono stati rimossi dalle porte sullo switch e lo switch è pronto per la cancellazione della configurazione.

- b. Entra in modalità privilegio:

```
(cs2)> enable
(cs2)#
```

- c. Copia e incolla i seguenti comandi per rimuovere la precedente configurazione RCF (a seconda della precedente versione RCF utilizzata, alcuni comandi potrebbero generare un errore se una particolare impostazione non è presente):

```

clear config interface 0/1-0/56
y
clear config interface lag 1
y
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no class-map CLUSTER
no class-map HA
no class-map RDMA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit

```

d. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
(cs2)# write memory
```

```
This operation may take a few minutes.  
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

e. Eseguire un riavvio dello switch:

```
(cs2)# reload
```

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

f. Accedere nuovamente allo switch tramite SSH per completare l'installazione RCF.

7. Notare quanto segue:

- a. Se sullo switch sono state installate licenze di porta aggiuntive, è necessario modificare l'RCF per configurare le porte con licenza aggiuntive. Vedere ["Attiva le porte appena concesse in licenza"](#) per i dettagli.
- b. Registrare tutte le personalizzazioni apportate nel precedente RCF e applicarle al nuovo RCF. Ad esempio, impostando la velocità delle porte o codificando la modalità FEC.

EFOS versione 3.12.x e successive

1. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Questo esempio mostra come SFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs2:

```
(cs2)# copy tftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..... TFTP
Set Server IP..... 172.19.2.1
Path..... /
Filename..... BES-53248_RCF_v1.9-Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... reference-config.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifica che lo script sia stato scaricato e salvato con il nome file che gli hai assegnato:

```
script list
```

```
(cs2)# script list

Configuration Script Name          Size(Bytes)  Date of
Modification
-----
reference-config.scr               2680        2024 05 31
21:54:22
2 configuration script(s) found.
2042 Kbytes free.
```

2. Applica lo script allo switch:

```
script apply
```

```
(cs2)# script apply reference-config.scr
```

```
Are you sure you want to apply the configuration script? (y/n) y
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
Configuration script 'reference-config.scr' applied.
```

Tutte le altre versioni EFOS

1. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Questo esempio mostra come SFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt  
nvrn:script BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Remote Password:**
```

```
Mode..... SFTP
```

```
Set Server IP..... 172.19.2.1
```

```
Path..... //tmp/
```

```
Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.txt
```

```
Data Type..... Config Script
```

```
Destination Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.scr
```

```
Management access will be blocked for the duration of the transfer
```

```
Are you sure you want to start? (y/n) y
```

```
SFTP Code transfer starting...
```

```
File transfer operation completed successfully.
```

1. Verifica che lo script sia stato scaricato e salvato nel nome file che gli hai assegnato:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
----- -----	-----	
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

```
1 configuration script(s) found.
```

2. Applica lo script allo switch:

```
script apply
```

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Are you sure you want to apply the configuration script? (y/n) y
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. Esaminare l'output del banner dal `show clibanner` comando. È necessario leggere e seguire queste istruzioni per verificare la corretta configurazione e il corretto funzionamento dello switch.

Mostra esempio

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename   : BES-53248-RCF-v1.9-Cluster.txt
```

```
Date       : 10-26-2022
```

```
Version    : v1.9
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

```
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms  
of port
```

```
speed:
```

```
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-  
40, 41-44,  
45-48
```

```
The port speed should be the same (10GbE or 25GbE) across all ports  
in a 4-port
```

```
group
```

```
- If additional licenses are purchased, follow the 'Additional Node  
Ports
```

```
activated with Licenses' section for instructions
```

```
- If SSH is active, it will have to be re-enabled manually after  
'erase
```

```
startup-config'
```

```
command has been executed and the switch rebooted
```

2. Sullo switch, verificare che le porte con licenza aggiuntive vengano visualizzate dopo l'applicazione dell'RCF:

```
show port all | exclude Detach
```

Mostra esempio

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

3. Verifica sullo switch che le modifiche siano state apportate:

```
show running-config
```

```
(cs2)# show running-config
```

4. Salvare la configurazione in esecuzione in modo che diventi la configurazione di avvio quando si riavvia lo switch:

```
write memory
```

```
(cs2)# write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

5. Riavviare lo switch e verificare che la configurazione in esecuzione sia corretta:

```
reload
```

```
(cs2)# reload
```

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

```
System will now restart!
```

6. Sullo switch del cluster cs2, richiamare le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono collegate ai nodi ONTAP :

```
(cs2)> enable
```

```
(cs2)# configure
```

```
(cs2) (Config)# interface 0/1-0/16
```

```
(cs2) (Interface 0/1-0/16)# no shutdown
```

```
(cs2) (Interface 0/1-0/16)# exit
```

```
(cs2) (Config)#
```

7. Verificare le porte sullo switch cs2:

```
show interfaces status all | exclude Detach
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Verificare che le porte e0b 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					
e0b	Cluster	Cluster		up	9000	auto/100000
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/100000
healthy	false					
e0b	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	0/2
BES-53248			
	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp			
	e0a	cs1	0/1
BES-53248			
	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp			
	e0a	cs1	0/4
BES-53248			
	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp			
	e0a	cs1	0/3
BES-53248			
	e0b	cs2	0/2
BES-53248			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-is-operational true
Switch                               Type                Address             Model
-----
cs1                                  cluster-network     10.228.143.200      BES-
53248
    Serial Number: QTWCU22510008
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP

cs2                                  cluster-network     10.228.143.202      BES-
53248
    Serial Number: QTWCU22510009
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

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

L'esempio seguente utilizza l'output dell'esempio di interfaccia:

```
(cs1)> enable
(cs1)# configure
(cs1) (Config)# interface 0/1-0/16
(cs1) (Interface 0/1-0/16)# shutdown
```

2. 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	e0a	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	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	e0a	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
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. Ripetere i passaggi da 4 a 19 sullo switch cs1.

5. Abilita il ripristino automatico sui LIF del cluster:

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

6. Riavviare lo switch cs1. Ciò fa sì che i LIF del cluster tornino alle loro porte di origine. È possibile ignorare gli eventi "porte cluster inattive" segnalati sui nodi durante il riavvio dello switch.

```
(cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved! System will now restart!
```

Passaggio 3: verificare la configurazione

1. Sullo switch cs1, verificare che le porte dello switch connesse alle porte del cluster siano **attive**:

```
show interfaces status all | exclude Detach
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Verificare che l'ISL tra gli switch cs1 e cs2 sia funzionante:

```
show port-channel 1/1
```

Mostra esempio

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----
0/55     actor/long      Auto      True
         partner/long
0/56     actor/long      Auto      True
         partner/long
```

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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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 `show` comando per visualizzare i dettagli.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
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)

```

1. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver installato l'RCF, puoi [abilita SSH](#).

Abilita SSH sugli switch cluster BES-53248

Se si utilizzano le funzionalità di monitoraggio dello stato dello switch Ethernet (CSHM) e di raccolta dei registri, è necessario generare le chiavi SSH e quindi abilitare SSH sugli switch del cluster.

Passi

1. Verificare che SSH sia disabilitato:

```
show ip ssh
```

Mostra esempio

```
(switch)# show ip ssh
```

SSH Configuration

```
Administrative Mode: ..... Disabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Disabled
SCP server Administrative Mode: ..... Disabled
```

- Se SSH non è disabilitato, disabilitarlo come segue:

```
no ip ssh server enable
```

```
no ip scp server enable
```



- Per EFOS 3.12 e versioni successive, è necessario l'accesso alla console poiché le sessioni SSH attive vengono perse quando SSH è disabilitato.
- Per EFOS 3.11 e versioni precedenti, le sessioni SSH correnti vengono mantenute aperte dopo aver disabilitato il server SSH.

+



Assicuratevi di disabilitare SSH prima di modificare le chiavi, altrimenti verrà segnalato un avviso sullo switch.

2. In modalità di configurazione, genera le chiavi SSH:

```
crypto key generate
```

Mostra esempio

```
(switch) # config

(switch) (Config) # crypto key generate rsa

Do you want to overwrite the existing RSA keys? (y/n): y

(switch) (Config) # crypto key generate dsa

Do you want to overwrite the existing DSA keys? (y/n): y

(switch) (Config) # crypto key generate ecdsa 521

Do you want to overwrite the existing ECDSA keys? (y/n): y
```

3. In modalità di configurazione, imposta l'autorizzazione AAA per la raccolta dei log ONTAP :

```
aaa authorization commands "noCmdAuthList" none
```

Mostra esempio

```
(switch) (Config) # aaa authorization commands "noCmdAuthList" none
(switch) (Config) # exit
```

4. Riattivare SSH/SCP.

Mostra esempio

```
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
```

5. Salvare queste modifiche nel file startup-config:

```
write memory
```

Mostra esempio

```
(switch)# write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.
Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

6. Crittografare le chiavi SSH (solo per la modalità **FIPS**):



Nella modalità FIPS, per motivi di sicurezza, le chiavi devono essere crittografate con una passphrase. In assenza di una chiave crittografata, l'applicazione non riesce ad avviarsi. Le chiavi vengono create e crittografate utilizzando i seguenti comandi:

Mostra esempio

```
(switch) configure  
(switch) (Config)# crypto key encrypt write rsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# crypto key encrypt write dsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# crypto key encrypt write ecdsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# end  
(switch)# write memory
```

This operation may take a few minutes.
Management interfaces will not be available during this time.
Are you sure you want to save? (y/n) **y**

Config file 'startup-config' created successfully.

Configuration Saved!

7. Riavviare lo switch:

```
reload
```

8. Verificare che SSH sia abilitato:

```
show ip ssh
```

Mostra esempio

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: ..... Enabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Enabled
SCP server Administrative Mode: ..... Enabled
```

Cosa succederà ora?

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

Ripristinare lo switch del cluster BES-53248 ai valori predefiniti di fabbrica

Per ripristinare le impostazioni predefinite di fabbrica dello switch cluster BES-53248, è necessario cancellare le impostazioni dello switch BES-53248.

Informazioni su questo compito

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

Passi

1. Passare al prompt dei comandi con privilegi elevati.

```
(cs2)> enable
(cs2)#
```

2. Cancella la configurazione di avvio.

```
erase startup-config
```

```
(cs2)# erase startup-config
```

```
Are you sure you want to clear the configuration? (y/n) y
```

3. Riavviare lo switch.

```
(cs2)# reload
```

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



Se il sistema chiede se salvare la configurazione non salvata o modificata prima di ricaricare lo switch, selezionare **No**.

1. Attendi che lo switch si ricarichi, quindi accedi allo switch.

L'utente predefinito è "admin" e non è impostata alcuna password. Viene visualizzato un messaggio simile al seguente:

```
(Routing) >
```

Aggiorna lo switch

Flusso di lavoro di aggiornamento per gli switch cluster BES-53248

Seguire questi passaggi per aggiornare il software EFOS e i file di configurazione di riferimento (RCF) sugli switch cluster Broadcom BES-54328, se applicabile.

1

"Aggiorna la tua versione EFOS"

Scaricare e installare il software Ethernet Fabric OS (EFOS) sullo switch cluster BES-53248.

2

"Aggiorna la tua versione RCF"

Aggiornare l'RCF sullo switch cluster BES-53248, quindi verificare le porte per una licenza aggiuntiva dopo l'applicazione dell'RCF.

3

"Verificare la rete del cluster ONTAP dopo l'aggiornamento"

Verificare lo stato di salute della rete cluster ONTAP dopo un aggiornamento del software EFOS o RCF per gli switch cluster BES-53248.

Aggiorna il software EFOS

Per aggiornare il software EFOS sullo switch cluster BES-53248, seguire questi

passaggi.

Il software EFOS include una serie di funzionalità e protocolli di rete avanzati per lo sviluppo di sistemi infrastrutturali Ethernet e IP. Questa architettura software è adatta a qualsiasi dispositivo organizzativo di rete che utilizzi applicazioni che richiedono un'ispezione o una separazione completa dei pacchetti.

Preparati per l'aggiornamento

Prima di iniziare

- Scarica il software Broadcom EFOS applicabile per i tuoi switch cluster da "[Supporto per switch Ethernet Broadcom](#)" sito.
- Rivedere le seguenti note relative alle versioni EFOS.

Nota quanto segue:

- Quando si esegue l'aggiornamento da EFOS 3.4.xx a EFOS 3.7.xx o versione successiva, lo switch deve eseguire EFOS 3.4.4.6 (o versione successiva 3.4.xx). Se si utilizza una versione precedente a questa, aggiornare prima lo switch a EFOS 3.4.4.6 (o versione successiva 3.4.xx), quindi aggiornare lo switch a EFOS 3.7.xx o versione successiva.
- La configurazione per EFOS 3.4.xx e 3.7.xx o versioni successive è diversa. Per modificare la versione EFOS da 3.4.xx a 3.7.xx o successiva, o viceversa, è necessario ripristinare le impostazioni predefinite di fabbrica e (ri)applicare i file RCF per la versione EFOS corrispondente. Questa procedura richiede l'accesso tramite la porta della console seriale.
- A partire dalla versione EFOS 3.7.xx o successiva, è disponibile una versione non conforme a FIPS e una conforme a FIPS. Quando si passa da una versione non conforme a FIPS a una conforme a FIPS o viceversa, si applicano passaggi diversi. La modifica di EFOS da una versione non conforme a FIPS a una conforme a FIPS o viceversa ripristinerà le impostazioni predefinite di fabbrica dello switch. Questa procedura richiede l'accesso tramite la porta della console seriale.

Procedura	Versione EFOS corrente	Nuova versione EFOS	Passi di alto livello
Passaggi per aggiornare EFOS tra due versioni (non) conformi a FIPS	3.4.x.x	3.4.x.x	Aggiorna la nuova immagine EFOS utilizzando Metodo 1: Aggiorna EFOS . Le informazioni sulla configurazione e sulla licenza vengono conservate.

3.4.4.6 (o versione successiva 3.4.xx)	3.7.xx o versione successiva non conforme a FIPS	Aggiorna EFOS utilizzando Metodo 1: Aggiorna EFOS . Ripristinare le impostazioni predefinite di fabbrica dello switch e applicare il file RCF per EFOS 3.7.xx o versioni successive.	3.7.xx o versione successiva non conforme a FIPS
3.4.4.6 (o versione successiva 3.4.xx)	Eseguire il downgrade di EFOS utilizzando Metodo 1: Aggiorna EFOS . Ripristinare l'interruttore alle impostazioni predefinite di fabbrica e applicare il file RCF per EFOS 3.4.xx	3.7.xx o versione successiva non conforme a FIPS	
Aggiorna la nuova immagine EFOS utilizzando Metodo 1: Aggiorna EFOS . Le informazioni sulla configurazione e sulla licenza vengono conservate.	3.7.xx o versione successiva conforme a FIPS	3.7.xx o versione successiva conforme a FIPS	Aggiorna la nuova immagine EFOS utilizzando Metodo 1: Aggiorna EFOS . Le informazioni sulla configurazione e sulla licenza vengono conservate.
Passaggi per l'aggiornamento a/da una versione EFOS conforme a FIPS	Non conforme a FIPS	Conforme a FIPS	Aggiornamento dell'immagine EFOS utilizzando Metodo 2: Aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE . La configurazione dello switch e le informazioni sulla licenza andranno perse.

Per verificare se la tua versione di EFOS è conforme o non conforme a FIPS, usa `show fips status` comando. Negli esempi seguenti, **IP_switch_a1** utilizza EFOS conforme a FIPS e **IP_switch_a2** utilizza EFOS non conforme a FIPS.

- Sullo switch **IP_switch_a1** (EFOS conforme a FIPS):

IP_switch_a1 # show fips status

System running in FIPS mode

- Sullo switch **IP_switch_a2** (EFOS non conforme a FIPS):

IP_switch_a2 # show fips status

^
% Invalid input detected at ^ marker.

Aggiorna il software

Utilizzare uno dei seguenti metodi:

- [Metodo 1: Aggiorna EFOS](#). Da utilizzare nella maggior parte dei casi (vedere la tabella sopra).
- [Metodo 2: Aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE](#). Utilizzare se una versione di EFOS è conforme a FIPS e l'altra non lo è.



Aggiornare EFOS su uno switch alla volta per garantire il funzionamento continuo della rete cluster.

Metodo 1: Aggiorna EFOS

Per aggiornare il software EFOS, procedere come segue.



Si noti che dopo l'aggiornamento degli switch cluster BES-53248 da EFOS 3.3.xx o 3.4.xx a EFOS 3.7.0.4 o 3.8.0.2, i collegamenti inter-switch (ISL) e i canali delle porte vengono contrassegnati nello stato **Down**. Si tratta di un comportamento previsto ed è possibile continuare l'aggiornamento in tutta sicurezza, a meno che non si riscontrino problemi con i LIF di ripristino automatico. Consultare l'articolo della Knowledge Base: ["BES-53248 Cluster Switch NDU non è riuscito ad aggiornare a EFOS 3.7.0.4 e versioni successive"](#) per ulteriori dettagli.

Passi

1. Collegare lo switch cluster BES-53248 alla rete di gestione.
2. Utilizzare il `ping` comando per verificare la connettività al server che ospita EFOS, le licenze e il file RCF.

Questo esempio verifica che lo switch sia connesso al server all'indirizzo IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

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

3. Disabilitare il ripristino automatico sui LIF del cluster.

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

4. Visualizza le immagini di avvio per la configurazione attiva e di backup:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active  next-active
-----
1         3.7.0.4      3.4.4.6      3.7.0.4         3.7.0.4
```

5. Scarica il file immagine sullo switch.

Copiando il file immagine nell'immagine di backup, al riavvio tale immagine stabilisce la versione EFOS in esecuzione, completando l'aggiornamento.

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk backup
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.10.0.3.stk
Data Type..... Code
Destination Filename..... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...

File transfer operation completed successfully.
```

6. Visualizza le immagini di avvio per la configurazione attiva e di backup:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1         3.7.0.4      3.10.0.3           3.7.0.4           3.10.0.3
```

7. Avviare il sistema dalla configurazione di backup:

```
boot system backup
```

```
(cs2)# boot system backup
Activating image backup ..
```

8. Visualizza le immagini di avvio per la configurazione attiva e di backup:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active

1	3.10.0.3	3.10.0.3	3.10.0.3	3.10.0.3

9. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
write memory
```

Mostra esempio

```
(cs2)# write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) **y**

Config file 'startup-config' created successfully.

Configuration Saved!

10. Riavviare lo switch:

```
reload
```

Mostra esempio

```
(cs2)# reload
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
System will now restart!
```

11. Effettua nuovamente l'accesso e verifica la nuova versione del software EFOS:

```
show version
```

Mostra esempio

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04  
Machine Type..... BES-53248A1,  
Machine Model..... BES-53248  
Serial Number..... QTFCU38260023  
Maintenance Level..... A  
Manufacturer..... 0xbc00  
Burned In MAC Address..... D8:C4:97:71:0F:40  
Software Version..... 3.10.0.3  
Operating System..... Linux 4.4.211-  
28a6fe76  
Network Processing Device..... BCM56873_A0  
CPLD Version..... 0xff040c03  
  
Additional Packages..... BGP-4  
..... QOS  
..... Multicast  
..... IPv6  
..... Routing  
..... Data Center  
..... OpEN API  
..... Prototype Open API
```

12. Ripetere i passaggi da 5 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 -vserver Cluster
```

Per ulteriori dettagli, vedere ["Ripristinare un LIF alla sua porta di origine"](#) .

Metodo 2: Aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE

È possibile eseguire i seguenti passaggi se una versione di EFOS è conforme a FIPS e l'altra non lo è. Questi passaggi possono essere utilizzati per aggiornare l'immagine EFOS 3.7.xx non FIPS o conforme a FIPS da ONIE se lo switch non riesce ad avviarsi.



Questa funzionalità è disponibile solo per EFOS 3.7.xx o versioni successive non conformi a FIPS.



Se si aggiorna EFOS tramite l'installazione del sistema operativo ONIE, la configurazione viene ripristinata ai valori predefiniti di fabbrica e le licenze vengono eliminate. Per ripristinare il normale funzionamento dello switch, è necessario configurare lo switch e installare le licenze e un RCF supportato.

Passi

1. Disabilitare il ripristino automatico sui LIF del cluster.

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

2. Avviare lo switch in modalità di installazione ONIE.

Durante l'avvio, seleziona ONIE quando vedi il prompt:

```

+-----+
| EFOS                                     |
| *ONIE                                  |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
+-----+

```

Dopo aver selezionato **ONIE**, l'interruttore si carica e ti presenta diverse scelte. Selezionare **Installa sistema operativo**.

```

+-----+
| *ONIE: Install OS                       |
| ONIE: Rescue                           |
| ONIE: Uninstall OS                     |
| ONIE: Update ONIE                      |
| ONIE: Embed ONIE                       |
| DIAG: Diagnostic Mode                   |
| DIAG: Burn-In Mode                     |
|                                         |
|                                         |
|                                         |
|                                         |
|                                         |
+-----+

```

Lo switch si avvia in modalità di installazione ONIE.

3. Interrompere la scoperta ONIE e configurare l'interfaccia Ethernet.

Quando viene visualizzato il seguente messaggio, premere **Invio** per richiamare la console ONIE:

```

Please press Enter to activate this console. Info: eth0: Checking
link... up.
ONIE:/ #

```



La scoperta ONIE continua e i messaggi vengono stampati sulla console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

4. Configurare l'interfaccia Ethernet e aggiungere il percorso utilizzando `ifconfig eth0 <ipAddress> netmask <netmask> up` e `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

5. Verificare che il server che ospita il file di installazione ONIE sia raggiungibile:

ping

Mostra esempio

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

6. Installa il nuovo software dello switch:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

Mostra esempio

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Il software installa e poi riavvia lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione EFOS.

7. Verificare che il nuovo software dello switch sia installato:

```
show bootvar
```

Mostra esempio

```
(cs2)# show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
-----
unit    active      backup    current-active  next-active
-----
1       3.7.0.4         3.7.0.4    3.7.0.4         3.10.0.3
(cs2) #
```

8. Completare l'installazione. Lo switch si riavvia senza alcuna configurazione applicata e ripristina le impostazioni predefinite di fabbrica. Per riconfigurare lo switch, completare i seguenti passaggi:
- "[Installa le licenze](#)"
 - "[Installare l'RCF](#)"
 - "[Abilita SSH](#)"
 - "[Abilita la raccolta dei log](#)"

e. ["Configurare SNMPv3 per il monitoraggio"](#)

9. Ripetere i passaggi da 2 a 8 sullo switch cs1.

10. Abilita il ripristino automatico sui LIF del cluster.

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

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

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

Per ulteriori dettagli, vedere ["Ripristinare un LIF alla sua porta di origine"](#).

Aggiornare il file di configurazione di riferimento (RCF)

È possibile aggiornare il file di configurazione di riferimento (RCF) dopo aver aggiornato lo switch cluster BES-53248 EFOS e dopo aver applicato eventuali nuove licenze.

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).
- Il file RCF corrente, disponibile da ["Switch cluster Broadcom"](#) pagina.
- Una configurazione di avvio nell'RCF che riflette le immagini di avvio desiderate, necessaria se si installa solo EFOS e si mantiene la versione RCF corrente. 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.
- Una connessione della console allo switch, necessaria quando si installa l'RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.

Documentazione suggerita

- Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedi il ["Scarica il software EFOS"](#) pagina. Si noti che possono esserci dipendenze tra la sintassi dei comandi nella RCF e quella presente nelle versioni di EFOS.
- Fare riferimento alle guide software e di aggiornamento appropriate disponibili sul ["Broadcom"](#) sito per la documentazione completa sulle procedure di upgrade e downgrade dello switch BES-53248.

Informazioni sugli esempi

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

- I nomi dei due switch BES-53248 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.

Informazioni su questo compito

La procedura richiede l'uso sia dei comandi ONTAP sia dei comandi dello switch Broadcom; 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 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, utilizzare l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) . Se è necessario cancellare completamente le impostazioni dello switch, sarà necessario eseguire nuovamente la configurazione di base. È necessario connettersi allo switch tramite la console seriale, poiché una cancellazione completa della configurazione reimposta la configurazione della rete di gestione.

Passaggio 1: Prepararsi all'aggiornamento

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.

Il seguente comando sopprime la creazione automatica dei casi per due ore:

```
system node autosupport invoke -node * -type all -message MAINT=2h
```

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (`*>`).

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                0/2        BES-
53248
          e0b    cs2                0/2        BES-
53248
cluster1-02/cdp
          e0a    cs1                0/1        BES-
53248
          e0b    cs2                0/1        BES-
53248
cluster1-03/cdp
          e0a    cs1                0/4        BES-
53248
          e0b    cs2                0/4        BES-
53248
cluster1-04/cdp
          e0a    cs1                0/3        BES-
53248
          e0b    cs2                0/3        BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```
Ignore
```

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

b. 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	
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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Disabilitare il ripristino automatico sui LIF del cluster.

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

Passaggio 2: configurare le porte

1. Sullo switch cs2, confermare l'elenco delle porte connesse ai nodi nel cluster.

```
show isdp neighbor
```

2. Sullo switch cs2, chiudere le porte collegate alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono collegate ai nodi ONTAP :

```
(cs2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)#
```

3. Verificare che i LIF del cluster siano stati migrati alle 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::*>				

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
```

5. Se non lo hai già fatto, salva la configurazione corrente dello switch copiando l'output del seguente comando in un file di registro:

```
show running-config
```

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



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Per cancellare le impostazioni dello switch è necessario essere connessi allo switch tramite la console seriale. Questo requisito è facoltativo se hai utilizzato l'articolo della Knowledge Base ["Come cancellare la configurazione su uno switch di interconnessione Broadcom mantenendo la connettività remota"](#) per cancellare la configurazione in anticipo.



La cancellazione della configurazione non elimina le licenze.

- a. Accedi allo switch tramite SSH.

Procedere solo quando tutti i cluster LIF sono stati rimossi dalle porte sullo switch e lo switch è pronto per la cancellazione della configurazione.

- b. Entra in modalità privilegio:

```
(cs2)> enable
(cs2) #
```

- c. Copia e incolla i seguenti comandi per rimuovere la precedente configurazione RCF (a seconda della precedente versione RCF utilizzata, alcuni comandi potrebbero generare un errore se una particolare impostazione non è presente):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```

```

configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDstA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
show running-config

```

d. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
write memory
```

```
(cs2)# write memory
```

```
This operation may take a few minutes.  
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Config file 'startup-config' created successfully.  
Configuration Saved!
```

e. Eseguire un riavvio dello switch:

```
reload
```

```
(cs2)# reload
```

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

a. Accedere nuovamente allo switch tramite SSH per completare l'installazione RCF.

7. Notare quanto segue:

- a. Se sullo switch sono state installate licenze di porta aggiuntive, è necessario modificare l'RCF per configurare le porte con licenza aggiuntive. Vedere "[Attiva le porte appena concesse in licenza](#)" per i dettagli. Tuttavia, quando si esegue l'aggiornamento a RCF 1.12 o versioni successive, le modifiche non sono più necessarie perché tutte le interfacce sono ora preconfigurate.
- b. Registrare tutte le personalizzazioni apportate nel precedente RCF e applicarle al nuovo RCF. Ad esempio, impostando la velocità delle porte o codificando la modalità FEC.

EFOS versione 3.12.x e successive

1. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Questo esempio mostra come SFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs2:

```
(cs2)# copy sftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..... TFTP
Set Server IP..... 172.19.2.1
Path..... /
Filename..... BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... reference-config.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Verifica che lo script sia stato scaricato e salvato con il nome file che gli hai assegnato:

```
script list
```

```
(cs2)# script list

Configuration Script Name          Size(Bytes)   Date of
Modification
-----
reference-config.scr               2680          2024 05 31
21:54:22
2 configuration script(s) found.
2042 Kbytes free.
```

2. Applica lo script allo switch:

```
script apply
```

```
(cs2)# script apply reference-config.scr
```

```
Are you sure you want to apply the configuration script? (y/n) y
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
Configuration script 'reference-config.scr' applied.
```

Tutte le altre versioni EFOS

1. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Questo esempio mostra come SFTP viene utilizzato per copiare un RCF nel bootflash sullo switch cs2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt  
nvram:script BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Remote Password:**
```

```
Mode..... SFTP
```

```
Set Server IP..... 172.19.2.1
```

```
Path..... //tmp/
```

```
Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.txt
```

```
Data Type..... Config Script
```

```
Destination Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.scr
```

```
Management access will be blocked for the duration of the transfer
```

```
Are you sure you want to start? (y/n) y
```

```
SFTP Code transfer starting...
```

```
File transfer operation completed successfully.
```

1. Verifica che lo script sia stato scaricato e salvato nel nome file che gli hai assegnato:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
-----	-----	
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

```
1 configuration script(s) found.
```

2. Applica lo script allo switch:

```
script apply
```

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Are you sure you want to apply the configuration script? (y/n) y
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

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

```
show clibanner
```

Mostra esempio

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename  : BES-53248-RCF-v1.9-Cluster.txt
```

```
Date      : 10-26-2022
```

```
Version   : v1.9
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

```
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms  
of port
```

```
speed:
```

```
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-  
40, 41-44,  
45-48
```

```
The port speed should be the same (10GbE or 25GbE) across all ports  
in a 4-port
```

```
group
```

```
- If additional licenses are purchased, follow the 'Additional Node  
Ports
```

```
activated with Licenses' section for instructions
```

```
- If SSH is active, it will have to be re-enabled manually after  
'erase
```

```
startup-config'
```

```
command has been executed and the switch rebooted
```

2. Sullo switch, verificare che le porte con licenza aggiuntive vengano visualizzate dopo l'applicazione dell'RCF:

```
show port all | exclude Detach
```

Mostra esempio

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

3. Verificare sullo switch che le modifiche siano state apportate.

```
show running-config
```

4. Salvare la configurazione in esecuzione in modo che diventi la configurazione di avvio quando si riavvia lo switch:

```
write memory
```

Mostra esempio

```
(cs2)# write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
```

5. Riavviare lo switch e verificare che la configurazione in esecuzione sia corretta.

```
reload
```

```
(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

6. Sullo switch del cluster cs2, richiamare le porte connesse alle porte del cluster dei nodi.

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Config)# exit
```

7. Salvare la configurazione in esecuzione nella configurazione di avvio:

```
write memory
```

Mostra esempio

```
(cs2)# write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
```

8. Verificare le porte sullo switch cs2:

```
show interfaces status all | exclude Detach
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Verificare che le porte e0b 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					
e0b	Cluster	Cluster		up	9000	auto/100000
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/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

b. Verificare lo stato di integrità dello switch dal cluster:

```
network device-discovery show
```

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

cluster1-01/cdp			
	e0a	cs1	0/2
BES-53248			
	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp			
	e0a	cs1	0/1
BES-53248			
	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp			
	e0a	cs1	0/4
BES-53248			
	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp			
	e0a	cs1	0/3
BES-53248			
	e0b	cs2	0/2
BES-53248			

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Ripetere i passaggi da 1 a 20 sullo switch cs1.
2. Abilita il ripristino automatico sui LIF del cluster:

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

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

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

Per ulteriori dettagli, vedere ["Ripristinare un LIF alla sua porta di origine"](#) .

Passaggio 3: verificare la configurazione

1. Sullo switch cs1, verificare che le porte dello switch connesse alle porte del cluster siano **attive**:

```
show interfaces status all
```

Mostra esempio

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Verificare che l'ISL tra gli switch cs1 e cs2 sia funzionante:

```
show port-channel 1/1
```

Mostra esempio

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----  -
0/55     actor/long    Auto      True
         partner/long
0/56     actor/long    Auto      True
         partner/long
```

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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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 `show` comando per visualizzare i dettagli.

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
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)

```

1. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Verificare la rete del cluster ONTAP dopo un aggiornamento del software EFOS o RCF degli switch del cluster BES-53248

È possibile utilizzare i seguenti comandi per verificare lo stato della rete cluster ONTAP dopo un aggiornamento del software EFOS o RCF per gli switch cluster BES-53248.

Passi

1. Visualizzare le informazioni sulle porte di rete sul cluster utilizzando il comando:

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

Link`deve avere il valore `up E Health Status deve essere healthy.

Mostra esempio

L'esempio seguente mostra l'output del comando:

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

Node: node1

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: node2

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							

2. Per ogni LIF, verificare che Is Home È true E Status Admin/Oper È up su entrambi i nodi, utilizzando il comando:

```
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				
	node1_clus1	up/up	169.254.217.125/16	node1
e0a	true			
	node1_clus2	up/up	169.254.205.88/16	node1
e0b	true			
	node2_clus1	up/up	169.254.252.125/16	node2
e0a	true			
	node2_clus2	up/up	169.254.110.131/16	node2
e0b	true			

3. Verificare che il Health Status di ogni nodo è true utilizzando il comando:

```
cluster show
```

Mostra esempio

```
cluster1::> cluster show
```

Node	Health	Eligibility	Epsilon

node1	true	true	false
node2	true	true	false

Cosa succederà ora?

Dopo aver confermato l'aggiornamento del software EFOS o RCF, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Migrare gli switch

Migrazione degli switch cluster CN1610 agli switch cluster BES-53248

Per migrare gli switch cluster CN1610 in un cluster verso switch cluster BES-53248 supportati da Broadcom, rivedere i requisiti di migrazione e quindi seguire la procedura di

migrazione.

Sono supportati i seguenti switch cluster:

- CN1610
- BES-53248

Requisiti di revisione

Verifica che la tua configurazione soddisfi i seguenti requisiti:

- Alcune porte degli switch BES-53248 sono configurate per funzionare a 10 GbE.
- La connettività 10GbE dai nodi agli switch cluster BES-53248 è stata pianificata, migrata e documentata.
- Il cluster è perfettamente funzionante (non dovrebbero esserci errori nei log o problemi simili).
- La personalizzazione iniziale degli switch BES-53248 è completa, in modo che:
 - Gli switch BES-53248 eseguono l'ultima versione consigliata del software EFOS.
 - I file di configurazione di riferimento (RCF) sono stati applicati agli switch.
 - Sui nuovi switch vengono configurate tutte le personalizzazioni del sito, come DNS, NTP, SMTP, SNMP e SSH.

Connessioni dei nodi

Gli switch del cluster supportano le seguenti connessioni di nodo:

- NetApp CN1610: porte da 0/1 a 0/12 (10GbE)
- BES-53248: porte 0/1-0/16 (10GbE/25GbE)



È possibile attivare porte aggiuntive acquistando licenze di porta.

porte ISL

Gli switch del cluster utilizzano le seguenti porte di collegamento inter-switch (ISL):

- NetApp CN1610: porte da 0/13 a 0/16 (10GbE)
- BES-53248: porte 0/55-0/56 (100GbE)

IL "[Universe hardware NetApp](#)" contiene informazioni sulla compatibilità ONTAP , sul firmware EFOS supportato e sul cablaggio per gli switch cluster BES-53248. 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.

Cablaggio ISL

Il cablaggio ISL appropriato è il seguente:

- **Inizio:** Per CN1610 a CN1610 (SFP+ a SFP+), quattro cavi SFP+ in fibra ottica o rame a collegamento diretto.
- **Finale:** Per BES-53248 a BES-53248 (da QSFP28 a QSFP28), due transceiver ottici QSFP28/cavi a collegamento diretto in fibra o rame.

Migrare gli switch

Seguire questa procedura per migrare gli switch cluster CN1610 agli switch cluster BES-53248.

Informazioni sugli esempi

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

- Gli esempi utilizzano due nodi, ciascuno dei quali distribuisce due porte di interconnessione cluster da 10 GbE: `e0a` E `e0b` .
- Gli output dei comandi potrebbero variare a seconda delle diverse versioni del software ONTAP .
- Gli interruttori CN1610 da sostituire sono `CL1` E `CL2` .
- Gli switch BES-53248 per sostituire gli switch CN1610 sono `cs1` E `cs2` .
- I nodi sono `node1` E `node2` .
- Lo switch `CL2` viene sostituito prima da `cs2`, seguito da `cs1` e `CL1`.
- Gli switch BES-53248 sono precaricati con le versioni supportate di Reference Configuration File (RCF) e Ethernet Fabric OS (EFOS) con cavi ISL collegati alle porte 55 e 56.
- I nomi LIF del cluster sono `node1_clus1` E `node1_clus2` per il nodo 1 e `node2_clus1` E `node2_clus2` per il nodo 2.

Informazioni su questo compito

Questa procedura copre il seguente scenario:

- Il cluster inizia con due nodi collegati a due switch cluster CN1610.
- Lo switch CN1610 `CL2` è sostituito dallo switch BES-53248 `cs2`:
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Scollegare i cavi da tutte le porte del cluster su tutti i nodi connessi a `CL2`, quindi utilizzare cavi supportati per ricollegare le porte al nuovo switch cluster `cs2`.
- Lo switch CN1610 `CL1` è sostituito dallo switch BES-53248 `cs1`:
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Scollegare i cavi da tutte le porte del cluster su tutti i nodi connessi a `CL1`, quindi utilizzare cavi supportati per ricollegare le porte al nuovo switch del cluster `cs1`.



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.

Fase 1: Prepararsi alla migrazione

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.

Il seguente comando sopprime la creazione automatica dei casi per due ore:

```
cluster1::*> system node autosupport invoke -node * -type all -message  
MAINT=2h
```

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

Passaggio 2: configurare porte e cablaggio

1. Sui nuovi switch, verificare che l'ISL sia cablato e funzionante tra gli switch cs1 e cs2:

```
show port-channel
```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono **attive** sullo switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
(cs1) #
```

L'esempio seguente mostra che le porte ISL sono **attive** sullo switch cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
```

2. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster esistenti:

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

Mostra esempio

L'esempio seguente mostra quante interfacce di interconnessione cluster sono state configurate in ciascun nodo per ogni switch di interconnessione cluster:

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
node2	/cdp		
	e0a	CL1	0/2
CN1610			
	e0b	CL2	0/2
CN1610			
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	CL2	0/1
CN1610			

3. Determinare lo stato amministrativo o operativo per ciascuna interfaccia del cluster.

a. Verificare che tutte le porte del cluster siano up con un healthy stato:

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

Mostra esempio

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

Node: node1

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					

Node: node2

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					

b. Verificare che tutte le interfacce cluster (LIF) siano sulle rispettive 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					
		node1_clus1	up/up	169.254.209.69/16	node1
e0a	true				
		node1_clus2	up/up	169.254.49.125/16	node1
e0b	true				
		node2_clus1	up/up	169.254.47.194/16	node2
e0a	true				
		node2_clus2	up/up	169.254.19.183/16	node2
e0b	true				

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

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando: `system switch ethernet show -is-monitoring-enabled-operational true`

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

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			

```
cluster1::*>
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando: `system cluster-switch show -is-monitoring-enabled-operational true`

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

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			

```
cluster1::*>
```

1. Disabilitare il ripristino automatico sui LIF del cluster.

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

2. Sullo switch cluster CL2, spegnere le porte connesse alle porte cluster dei nodi per eseguire il failover dei LIF del cluster:

```
(CL2)# configure
(CL2)(Config)# interface 0/1-0/16
(CL2)(Interface 0/1-0/16)# shutdown
(CL2)(Interface 0/1-0/16)# exit
(CL2)(Config)# exit
(CL2)#
```

3. Verificare che i LIF del cluster abbiano eseguito il failover sulle porte ospitate sullo switch del cluster CL1. 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				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0a	false			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0a	false			

4. Verificare che il cluster sia integro:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

- 5. Spostare tutti i cavi di connessione dei nodi del cluster dal vecchio switch CL2 al nuovo switch cs2.
- 6. Conferma lo stato delle connessioni di rete spostate su cs2:

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

Mostra esempio

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

Node: node1

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: node2

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						

Tutte le porte del cluster che sono state spostate dovrebbero essere up .

7. Controllare le informazioni sui vicini sulle porte del 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			

node2	/cdp		
	e0a	CL1	0/2
CN1610			
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	cs2	0/1
53248			BES-

8. Verificare che le connessioni delle porte dello switch siano corrette dal punto di vista dello switch cs2:

```
cs2# show interface all
cs2# show isdp neighbors
```

9. Sullo switch cluster CL1, spegnere le porte connesse alle porte cluster dei nodi per eseguire il failover dei LIF del cluster:

```
(CL1)# configure
(CL1) (Config)# interface 0/1-0/16
(CL1) (Interface 0/1-0/16)# shutdown
(CL1) (Interface 0/13-0/16)# exit
(CL1) (Config)# exit
(CL1) #
```

Tutti i LIF del cluster eseguono il failover sullo switch cs2.

10. Verificare che i LIF del cluster abbiano eseguito il failover sulle 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				
	node1_clus1	up/up	169.254.209.69/16	node1
e0b	false			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0b	false			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

11. Verificare che il cluster sia integro:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

12. Spostare i cavi di collegamento del nodo cluster da CL1 al nuovo switch cs1.

13. Conferma lo stato delle connessioni di rete spostate su cs1:

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

Mostra esempio

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

Node: node1

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: node2

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						

Tutte le porte del cluster che sono state spostate dovrebbero essere up .

14. Controllare le informazioni sui vicini sulle porte del cluster:

```
network device-discovery show
```

Mostra esempio

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			

node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-
node2	/cdp		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-

15. Verificare che le connessioni delle porte dello switch siano corrette dal punto di vista dello switch cs1:

```
cs1# show interface all
cs1# show isdp neighbors
```

16. Verificare che l'ISL tra cs1 e cs2 sia ancora operativo:

```
show port-channel
```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono **attive** sullo switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
(cs1) #
```

L'esempio seguente mostra che le porte ISL sono **attive** sullo switch cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
```

17. Eliminare gli switch CN1610 sostituiti dalla tabella degli switch del cluster, se non vengono rimossi

automaticamente:

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, utilizzare il comando: `system switch ethernet delete -device device-name`

```
cluster::*> system switch ethernet delete -device CL1
cluster::*> system switch ethernet delete -device CL2
```

ONTAP 9.7 e precedenti

Per ONTAP 9.7 e versioni precedenti, utilizzare il comando: `system cluster-switch delete -device device-name`

```
cluster::*> system cluster-switch delete -device CL1
cluster::*> system cluster-switch delete -device CL2
```

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster.

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

2. Sullo switch cs2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle rispettive porte home.

```
cs2> enable
cs2# configure
cs2(config)# interface 0/1-0/16
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home (l'operazione potrebbe richiedere un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verificare che il cluster sia integro:

```
cluster show
```

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      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. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

```

cluster::*> system node autosupport invoke -node * -type all -message
MAINT=END

```

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Migrare a un ambiente cluster NetApp commutato

Se si dispone di un ambiente cluster a due nodi *senza switch*, è possibile migrare a un ambiente cluster a due nodi *con switch* utilizzando gli switch cluster BES-53248 supportati da Broadcom, che consentono di scalare oltre due nodi nel cluster.

Il processo di migrazione funziona per tutte le porte dei nodi del cluster che utilizzano porte ottiche o Twinax, ma non è supportato su questo switch se i nodi utilizzano porte RJ45 10GBASE-T integrate per le porte di rete del cluster.

Requisiti di revisione

Esaminare i seguenti requisiti per l'ambiente cluster.

- Tieni presente che la maggior parte dei sistemi richiede due porte di rete cluster dedicate su ciascun controller.
- Assicurarsi che lo switch cluster BES-53248 sia configurato come descritto in ["Sostituisci i requisiti"](#) prima di iniziare questo processo di migrazione.
- Per la configurazione senza switch a due nodi, assicurarsi che:
 - La configurazione switchless a due nodi è correttamente configurata e funzionante.
 - I nodi eseguono ONTAP 9.5P8 e versioni successive. Il supporto per le porte cluster 40/100 GbE inizia con il firmware EFOS versione 3.4.4.6 e successive.
 - Tutte le porte del cluster sono nello stato **attivo**.
 - Tutte le interfacce logiche del cluster (LIF) sono nello stato **attivo** e sulle loro porte home.
- Per la configurazione dello switch cluster BES-53248 supportato da Broadcom, assicurarsi che:
 - Lo switch cluster BES-53248 è completamente funzionante su entrambi gli switch.
 - Entrambi gli switch dispongono di connettività di rete di gestione.
 - È disponibile l'accesso alla console per gli switch del cluster.
 - Le connessioni tra switch e nodi BES-53248 utilizzano cavi Twinax o in fibra.

IL ["Universe hardware NetApp"](#) contiene informazioni sulla compatibilità ONTAP , sul firmware EFOS supportato e sul cablaggio per gli switch BES-53248. 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.

- I cavi Inter-Switch Link (ISL) sono collegati alle porte 0/55 e 0/56 su entrambi gli switch BES-53248.
- La personalizzazione iniziale di entrambi gli switch BES-53248 è completa, in modo che:
 - Gli switch BES-53248 utilizzano la versione software più recente.
 - Gli switch BES-53248 dispongono di licenze di porta opzionali installate, se acquistate.
 - I file di configurazione di riferimento (RCF) vengono applicati agli switch.
- Sui nuovi switch vengono configurate tutte le personalizzazioni del sito (SMTP, SNMP e SSH).

Vincoli di velocità del gruppo di porte

- Le 48 porte 10/25GbE (SFP28/SFP+) sono combinate in 12 gruppi da 4 porte come segue: Porte 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 e 45-48.
- La velocità della porta SFP28/SFP+ deve essere la stessa (10 GbE o 25 GbE) su tutte le porte del gruppo a 4 porte.
- Se le velocità in un gruppo a 4 porte sono diverse, le porte dello switch non funzioneranno correttamente.

Migrare all'ambiente cluster

Informazioni sugli esempi

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

- I nomi degli switch BES-53248 sono `cs1` E `cs2` .

- I nomi degli SVM del cluster sono `node1` E `node2` .
- I nomi dei LIF sono `node1_clus1` E `node1_clus2` sul nodo 1, e `node2_clus1` E `node2_clus2` rispettivamente sul nodo 2.
- IL `cluster1::*>` il prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono `e0a` E `e0b` .

IL "[Universo hardware NetApp](#)" contiene le informazioni più recenti sulle porte cluster effettive per le tue piattaforme.

Fase 1: Prepararsi alla migrazione

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.

Il seguente comando sopprime la creazione automatica dei casi per due ore:

```
cluster1::*> system node autosupport invoke -node * -type all -message MAINT=2h
```

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

```
set -privilege advanced
```

Il prompt avanzato(`*>`) appare.

Passaggio 2: configurare porte e cablaggio

1. Disabilitare tutte le porte attivate rivolte verso il nodo (non le porte ISL) su entrambi i nuovi switch del cluster `cs1` e `cs2`.



Non è consentito disattivare le porte ISL.

L'esempio seguente mostra che le porte da 1 a 16 rivolte al nodo sono disabilitate sullo switch `cs1`:

```
(cs1)# configure  
(cs1) (Config)# interface 0/1-0/16  
(cs1) (Interface 0/1-0/16)# shutdown  
(cs1) (Interface 0/1-0/16)# exit  
(cs1) (Config)# exit
```

2. Verificare che l'ISL e le porte fisiche sull'ISL tra i due switch BES-53248 cs1 e cs2 siano attivi:

```
show port-channel
```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono attive sullo switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed     Active
-----
0/55     actor/long      100G Full  True
         partner/long
0/56     actor/long      100G Full  True
         partner/long
(cs1) #
```

L'esempio seguente mostra che le porte ISL sono attive sullo switch cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed     Active
-----
0/55     actor/long      100G Full  True
         partner/long
0/56     actor/long      100G Full  True
         partner/long
```

3. Visualizza l'elenco dei dispositivi vicini:

```
show isdp neighbors
```

Questo comando fornisce informazioni sui dispositivi collegati al sistema.

Mostra esempio

L'esempio seguente elenca i dispositivi adiacenti sullo switch cs1:

```
(cs1)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Holdtime	Capability	Platform	Port ID
cs2	0/55	176	R	BES-53248	0/55
cs2	0/56	176	R	BES-53248	0/56

L'esempio seguente elenca i dispositivi adiacenti sullo switch cs2:

```
(cs2)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Holdtime	Capability	Platform	Port ID
cs2	0/55	176	R	BES-53248	0/55
cs2	0/56	176	R	BES-53248	0/56

4. Verificare che tutte le porte del cluster siano attive:

```
network port show -ipSpace Cluster
```

Mostra esempio

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

Node: node1

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

Node: node2

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

5. Verificare che tutti i cluster LIF siano attivi e operativi:

```
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				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

6. Disabilitare il ripristino automatico sui LIF del cluster.

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

7. Scollegare il cavo dalla porta e0a del cluster sul nodo 1, quindi collegare e0a alla porta 1 sullo switch cs1 del cluster, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.

IL "[Universe hardware NetApp](#)" contiene maggiori informazioni sul cablaggio.

8. Scollegare il cavo dalla porta e0a del cluster sul nodo 2, quindi collegare e0a alla porta 2 sullo switch cs1 del cluster, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.

9. Abilitare tutte le porte rivolte verso il nodo sullo switch del cluster cs1.

L'esempio seguente mostra che le porte da 1 a 16 sono abilitate sullo switch cs1:

```
(cs1)# configure  
(cs1)(Config)# interface 0/1-0/16  
(cs1)(Interface 0/1-0/16)# no shutdown  
(cs1)(Interface 0/1-0/16)# exit  
(cs1)(Config)# exit
```

10. Verificare che tutte le porte del cluster siano attive:

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

Mostra esempio

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

Node: node1

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: node2

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						

11. Verificare che tutti i cluster LIF siano attivi e operativi:

```
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					
node1_clus1	up/up	169.254.209.69/16	node1	e0a	
true					
node1_clus2	up/up	169.254.49.125/16	node1	e0b	
true					
node2_clus1	up/up	169.254.47.194/16	node2	e0a	
true					
node2_clus2	up/up	169.254.19.183/16	node2	e0b	
true					

12. Visualizza informazioni sullo stato dei nodi nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

13. Scollegare il cavo dalla porta e0b del cluster sul nodo 1, quindi collegare e0b alla porta 1 sullo switch cs2 del cluster, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.
14. Scollegare il cavo dalla porta e0b del cluster sul nodo 2, quindi collegare e0b alla porta 2 sullo switch cs2 del cluster, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.
15. Abilitare tutte le porte rivolte verso il nodo sullo switch cluster cs2.

L'esempio seguente mostra che le porte da 1 a 16 sono abilitate sullo switch cs2:

```
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# no shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)# exit
```

16. Verificare che tutte le porte del cluster siano attive:

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

Mostra esempio

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

Node: node1

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: node2

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						

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster.

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

2. Sullo switch cs2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle rispettive porte home.

```
cs2> enable  
cs2# configure  
cs2(config)# interface 0/1-0/16  
cs2(config-if-range)# shutdown  
  
(Wait for 5-10 seconds before re-enabling the ports)  
  
cs2(config-if-range)# no shutdown  
  
(After executing the no shutdown command, the nodes detect the change  
and begin to auto-revert the cluster LIFs to their home ports)  
  
cs2(config-if-range)# exit  
cs2(config)# exit  
cs2#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home (l'operazione potrebbe richiedere un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verificare che tutte le interfacce siano visualizzate `true` per `Is Home` :

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



L'operazione potrebbe richiedere diversi minuti.

Mostra esempio

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

5. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
show isdp neighbors
```

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
(cs1)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Holdtime	Capability	Platform	Port ID
-----------	------	----------	------------	----------	---------

node1	0/1	175	H	FAS2750	e0a
node2	0/2	157	H	FAS2750	e0a
cs2	0/55	178	R	BES-53248	0/55
cs2	0/56	178	R	BES-53248	0/56

```
(cs2)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Holdtime	Capability	Platform	Port ID
-----------	------	----------	------------	----------	---------

node1	0/1	137	H	FAS2750	e0b
node2	0/2	179	H	FAS2750	e0b
cs1	0/55	175	R	BES-53248	0/55
cs1	0/56	175	R	BES-53248	0/56

6. Visualizza informazioni sui dispositivi di rete rilevati nel tuo 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			

node2	/cdp		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-

7. Verificare che le impostazioni siano disabilitate:

```
network options switchless-cluster show
```



Potrebbero essere necessari diversi minuti affinché il comando venga completato. Attendi l'annuncio "Scadenza della durata di 3 minuti".

IL false l'output nell'esempio seguente mostra che le impostazioni di configurazione sono disabilitate:

```
cluster1::*> network options switchless-cluster show
```

Enable Switchless Cluster: **false**

8. Verificare lo stato dei membri del nodo nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

9. 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	LIF
Loss				

node1				
	3/5/2022 19:21:18 -06:00		node1_clus2	node2_clus1
none				
	3/5/2022 19:21:20 -06:00		node1_clus2	node2_clus2
none				
node2				
	3/5/2022 19:21:18 -06:00		node2_clus2	node1_clus1
none				
	3/5/2022 19:21:20 -06:00		node2_clus2	node1_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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      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. Riporta il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Mostra esempio

```

cluster1::*> system node autosupport invoke -node * -type all
-messaggio MAINT=END

```

Per maggiori informazioni, vedere: ["Articolo della Knowledge Base NetApp : Come sopprimere la creazione automatica dei casi durante le finestre di manutenzione programmata"](#)

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituire gli interruttori

Requisiti di sostituzione

Prima di sostituire l'interruttore, assicurarsi che le seguenti condizioni siano soddisfatte nell'ambiente attuale e sull'interruttore sostitutivo.

Cluster esistente e infrastruttura di rete

Assicurarsi che:

- Il cluster esistente è stato verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
- Tutte le porte del cluster sono **attive**.
- Tutte le interfacce logiche del cluster (LIF) sono amministrativamente e operativamente **attive** e sulle loro porte home.
- L'ONTAP `cluster ping-cluster -node node1` il comando deve indicare che le impostazioni, `basic connectivity` `E larger than PMTU communication`, hanno successo su tutti i percorsi.

Interruttore cluster sostitutivo BES-53248

Assicurarsi che:

- La connettività della rete di gestione sullo switch sostitutivo è funzionante.
- L'accesso alla console per l'interruttore sostitutivo è pronto.
- Le connessioni dei nodi sono le porte da 0/1 a 0/16 con licenza predefinita.
- Tutte le porte Inter-Switch Link (ISL) sono disabilitate sulle porte 0/55 e 0/56.
- Il file di configurazione di riferimento desiderato (RCF) e l'immagine dello switch del sistema operativo EFOS vengono caricati sullo switch.
- La personalizzazione iniziale dello switch è completa, come dettagliato in ["Configurare lo switch cluster BES-53248"](#).

Tutte le personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengono copiate sul nuovo switch.

Abilita la registrazione della console

NetApp consiglia vivamente di abilitare la registrazione della console sui dispositivi utilizzati e di adottare le seguenti misure quando si sostituisce lo switch:

- Lasciare AutoSupport abilitato durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione di casi per tutta la durata della manutenzione. Vedi questo articolo della Knowledge Base ["SU92: Come sopprimere la creazione automatica dei casi durante le finestre di manutenzione programmata"](#) per ulteriori dettagli.
- Abilita la registrazione delle sessioni per tutte le sessioni CLI. Per istruzioni su come abilitare la registrazione della sessione, consultare la sezione "Registrazione dell'output della sessione" in questo articolo della Knowledge Base ["Come configurare PuTTY per una connettività ottimale ai sistemi ONTAP"](#).

Per maggiori informazioni

- ["Sito di supporto NetApp"](#)
- ["Hardware Universe NetApp"](#)

Sostituisci uno switch cluster BES-53248 supportato da Broadcom

Per sostituire uno switch cluster BES-53248 difettoso supportato da Broadcom in una rete cluster, seguire questi passaggi. Si tratta di una procedura non distruttiva (NDU).

Informazioni sugli esempi

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

- I nomi degli switch BES-53248 esistenti sono `cs1` E `cs2` .
- Il nome del nuovo switch BES-53248 è `newcs2` .
- I nomi dei nodi sono `node1` E `node2` .
- Le porte del cluster su ciascun nodo sono denominate `e0a` E `e0b` .
- I nomi LIF del cluster sono `node1_clus1` E `node1_clus2` per il nodo 1 e `node2_clus1` E `node2_clus2` per il nodo 2.
- La richiesta di modifiche a tutti i nodi del cluster è `cluster1::>`

Informazioni sulla topologia

Questa procedura si basa sulla seguente topologia di rete cluster:

Mostra topologia di esempio

cluster1::> network port show -ipspace Cluster

Node: node1

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: node2

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::> network interface show -vserver Cluster

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

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					

```
node2_clus1 up/up 169.254.47.194/16 node2 e0a
true
node2_clus2 up/up 169.254.19.183/16 node2 e0b
true
```

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	0/2	BES-
53248				
	e0b	cs2	0/2	BES-
53248				
node1	/cdp			
	e0a	cs1	0/1	BES-
53248				
	e0b	cs2	0/1	BES-
53248				

```
(cs1)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Port ID	Intf	Holdtime	Capability	Platform
node1 e0a	0/1	175	H	FAS2750
node2 e0a	0/2	152	H	FAS2750
cs2 0/55	0/55	179	R	BES-53248
cs2 0/56	0/56	179	R	BES-53248

```
(cs2)# show isdp neighbors
```

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

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Port ID	Intf	Holdtime	Capability	Platform
node1 e0b	0/1	129	H	FAS2750
node2 e0b	0/2	165	H	FAS2750
cs1 0/55	0/55	179	R	BES-53248
cs1 0/56	0/56	179	R	BES-53248

Passi

1. Rivedere il "[Requisiti di sostituzione](#)".
2. 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.

3. Installare il file di configurazione di riferimento (RCF) e l'immagine appropriati sullo switch, newcs2, ed effettuare le necessarie preparazioni del sito.

Se necessario, verificare, scaricare e installare le versioni appropriate del software RCF ed EFOS per il nuovo switch. Se hai verificato che il nuovo switch è configurato correttamente e non necessita di aggiornamenti del software RCF ed EFOS, continua con il passaggio 2.

- a. È possibile scaricare il software Broadcom EFOS applicabile per gli switch del cluster da ["Supporto per switch Ethernet Broadcom"](#) sito. Seguire i passaggi indicati nella pagina Download per scaricare il file EFOS per la versione del software ONTAP che si sta installando.
 - b. L'RCF appropriato è disponibile presso ["Switch cluster Broadcom"](#) pagina. Seguire i passaggi indicati nella pagina Download per scaricare il file RCF corretto per la versione del software ONTAP che si sta installando.
4. Sul nuovo switch, accedi come `admin` e chiudere tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da 1 a 16).



Se hai acquistato licenze aggiuntive per porte aggiuntive, chiudi anche queste porte.

Se lo switch che si sta sostituendo non è funzionante ed è spento, i LIF sui nodi del cluster dovrebbero aver già eseguito il failover sull'altra porta del cluster per ciascun nodo.



Non è richiesta alcuna password per entrare `enable` modalità.

Mostra esempio

```
User: admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2) (config)# interface 0/1-0/16
(newcs2) (interface 0/1-0/16)# shutdown
(newcs2) (interface 0/1-0/16)# exit
(newcs2) (config)# exit
(newcs2)#
```

5. Verificare che tutti i cluster LIF abbiano `auto-revert` abilitato:

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

Mostra topologia di esempio

```
cluster1::> network interface show -vserver Cluster -fields auto-revert
```

Logical Vserver	Interface	Auto-revert
Cluster	node1_clus1	true
Cluster	node1_clus2	true
Cluster	node2_clus1	true
Cluster	node2_clus2	true

6. Disattivare le porte ISL 0/55 e 0/56 sullo switch BES-53248 cs1:

Mostra topologia di esempio

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# shutdown
```

7. Rimuovere tutti i cavi dallo switch BES-53248 cs2, quindi collegarli alle stesse porte sullo switch BES-53248 newcs2.
8. Attivare le porte ISL 0/55 e 0/56 tra gli switch cs1 e newcs2, quindi verificare lo stato operativo del canale porta.

Lo stato del collegamento per il canale porta 1/1 dovrebbe essere **attivo** e tutte le porte membro dovrebbero essere impostate su True sotto l'intestazione Porta attiva.

Mostra esempio

Questo esempio abilita le porte ISL 0/55 e 0/56 e visualizza lo stato del collegamento per il canale porta 1/1 sullo switch cs1:

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# no shutdown
(cs1)(interface 0/55-0/56)# exit
(cs1)# show port-channel 1/1

Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed      Active
-----
0/55     actor/long     100G Full  True
         partner/long
0/56     actor/long     100G Full  True
         partner/long
```

9. Sul nuovo switch newcs2, riattivare tutte le porte connesse alle interfacce del cluster di nodi (porte da 1 a 16).



Se hai acquistato licenze aggiuntive per porte aggiuntive, chiudi anche queste porte.

Mostra esempio

```
User:admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2)(config)# interface 0/1-0/16
(newcs2)(interface 0/1-0/16)# no shutdown
(newcs2)(interface 0/1-0/16)# exit
(newcs2)(config)# exit
```

10. Verificare che la porta e0b sia **attiva**:

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

Mostra esempio

L'output dovrebbe essere simile al seguente:

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

Node: node1

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

Node: node2

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/auto  -
false
```

11. Sullo stesso nodo utilizzato nel passaggio precedente, attendi che il cluster LIF node1_clus2 sul nodo 1 venga ripristinato automaticamente.

Mostra esempio

In questo esempio, LIF node1_clus2 su node1 viene ripristinato correttamente se Is Home È true e la porta è e0b.

Il seguente comando visualizza informazioni sui LIF su entrambi i nodi. L'attivazione del primo nodo ha esito positivo se Is Home È true per entrambe le interfacce del cluster e mostrano le assegnazioni delle porte corrette, in questo esempio e0a E e0b sul nodo 1.

```
cluster::> network interface show -vserver Cluster
```

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0a	false			

12. Visualizza informazioni sui nodi in un cluster:

```
cluster show
```

Mostra esempio

Questo esempio mostra che lo stato di salute del nodo per node1 E node2 in questo cluster è true :

```
cluster1::> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	true
node2	true	true	true

13. Confermare la seguente configurazione di rete del cluster:

```
network port show
```

```
network interface show
```

Mostra esempio

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

```
Node: node1
```

```
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: node2
```

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2

```
e0a      true
          node2_clus2  up/up      169.254.19.183/16  node2
e0b      true
4 entries were displayed.
```

14. Verificare che la rete del cluster sia integra:

```
show isdp neighbors
```

Mostra esempio

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf      Holdtime    Capability    Platform      Port ID
-----
node1          0/1       175         H             FAS2750       e0a
node2          0/2       152         H             FAS2750       e0a
newcs2         0/55      179         R             BES-53248     0/55
newcs2         0/56      179         R             BES-53248     0/56

(newcs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Intf      Holdtime    Capability    Platform      Port ID
-----
node1          0/1       129         H             FAS2750       e0b
node2          0/2       165         H             FAS2750       e0b
cs1            0/55      179         R             BES-53248     0/55
cs1            0/56      179         R             BES-53248     0/56
```

15. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver sostituito gli interruttori, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituisci gli switch cluster Broadcom BES-53248 con connessioni switchless

È possibile migrare da un cluster con una rete di cluster commutata a uno in cui due nodi

sono collegati direttamente per ONTAP 9.3 e versioni successive.

Requisiti di revisione

Linee guida

Rivedere le seguenti linee guida:

- La migrazione a una configurazione cluster switchless a due nodi è un'operazione non distruttiva. La maggior parte dei sistemi ha due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per sistemi con un numero maggiore di porte di interconnessione cluster dedicate su ciascun nodo, ad esempio quattro, sei o otto.
- Non è possibile utilizzare la funzionalità di interconnessione del cluster senza switch con più di due nodi.
- Se si dispone di un cluster a due nodi esistente che utilizza switch di interconnessione cluster ed esegue ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

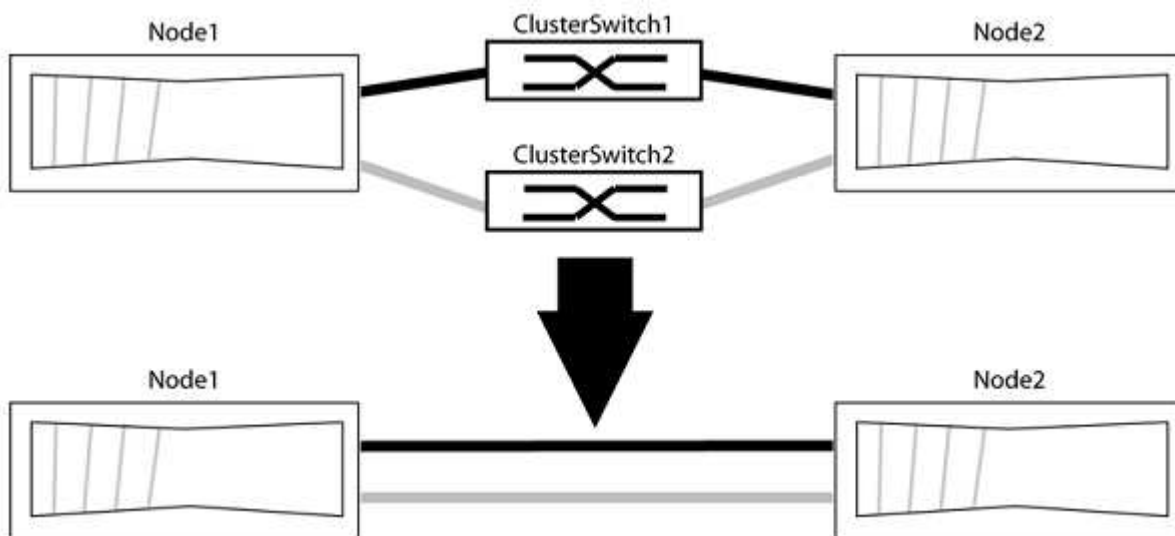
Assicurati di avere quanto segue:

- Un cluster sano costituito da due nodi collegati tramite switch di cluster. I nodi devono eseguire la stessa versione ONTAP .
- Ogni nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, ci sono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

Informazioni su questo compito

La seguente procedura rimuove gli switch del cluster in un cluster a due nodi e sostituisce ogni connessione allo switch con una connessione diretta al nodo partner.



Informazioni sugli esempi

Gli esempi nella seguente procedura mostrano nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse, poiché variano in base al sistema.

Fase 1: Prepararsi alla migrazione

1. Cambia il livello di privilegio in avanzato, inserendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato `*>` appare.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster switchless, abilitato per impostazione predefinita.

È possibile verificare che il rilevamento dei cluster switchless sia abilitato eseguendo il comando con privilegi avanzati:

```
network options detect-switchless-cluster show
```

Mostra esempio

Il seguente output di esempio mostra se l'opzione è abilitata.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Abilita rilevamento cluster senza switch" è `false`, contattare l'assistenza NetApp.

3. 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=<number_of_hours>h
```

Dove `h` è la durata della finestra di manutenzione in ore. Il messaggio avvisa il supporto tecnico di questa attività di manutenzione, in modo che possa sopprimere la creazione automatica dei casi durante la finestra di manutenzione.

Nell'esempio seguente, il comando sopprime la creazione automatica dei casi per due ore:

Mostra esempio

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Passaggio 2: configurare porte e cablaggio

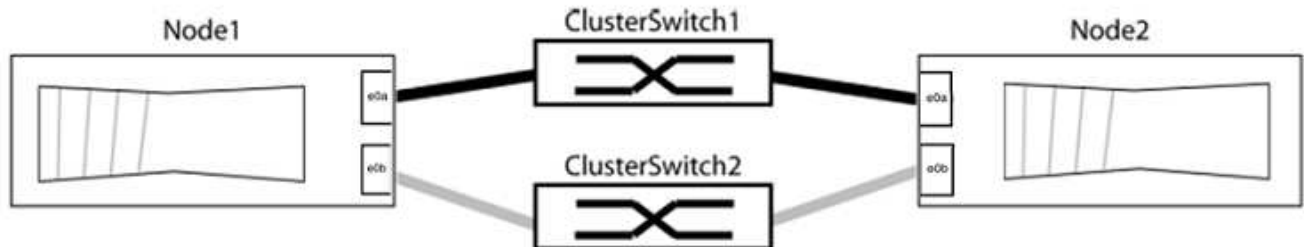
1. Organizzare le porte del cluster su ogni switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano al cluster switch 1 e le porte del cluster nel gruppo 2 vadano al cluster switch 2. Questi gruppi

saranno necessari più avanti nella procedura.

2. Identificare le porte del cluster e verificare lo stato e l'integrità del collegamento:

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

Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo è identificato come "nodo1:e0a" e "nodo2:e0a" e l'altro gruppo come "nodo1:e0b" e "nodo2:e0b". I nodi potrebbero utilizzare porte cluster diverse perché variano in base al sistema.



Verificare che le porte abbiano un valore di `up` per la colonna "Link" e un valore di `healthy` per la colonna "Stato di salute".

Mostra esempio

```
cluster::> network port show -ipspace Cluster
Node: node1

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: node2

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
4 entries were displayed.
```

3. Verificare che tutti i LIF del cluster siano sulle rispettive porte home.

Verificare che la colonna "is-home" sia true per ciascuno dei LIF del cluster:

```
network interface show -vserver Cluster -fields is-home
```

Mostra esempio

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-----  -
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se sono presenti LIF del cluster che non si trovano sulle loro porte home, ripristinare tali LIF sulle loro porte home:

```
network interface revert -vserver Cluster -lif *
```

4. Disabilitare il ripristino automatico per i LIF del cluster:

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

5. Verificare che tutte le porte elencate nel passaggio precedente siano connesse a uno switch di rete:

```
network device-discovery show -port cluster_port
```

La colonna "Dispositivo rilevato" dovrebbe contenere il nome dello switch del cluster a cui è connessa la porta.

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono collegate correttamente agli switch del cluster "cs1" e "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. 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	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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 cluster sia integro:

```
cluster ring show
```

Tutte le unità devono essere master o secondarie.

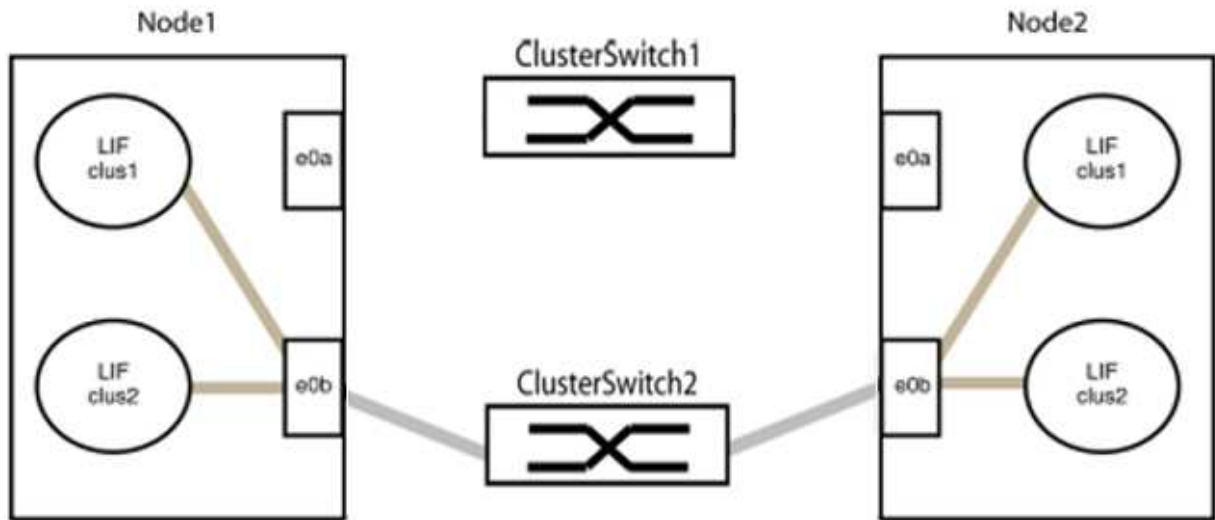
2. Impostare la configurazione senza switch per le porte del gruppo 1.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 1 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

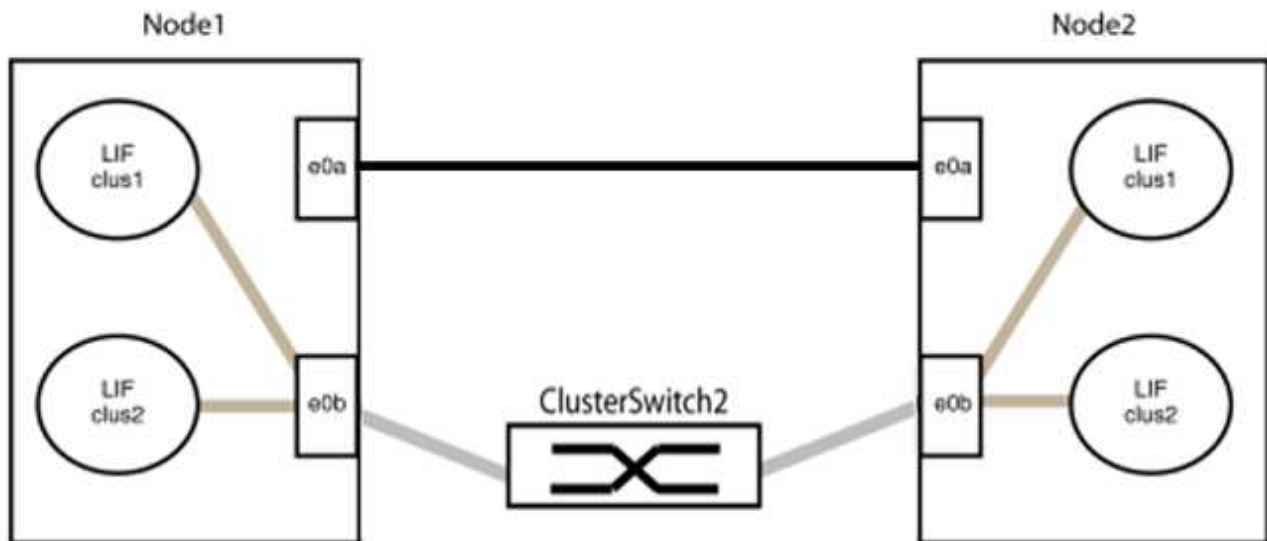
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 1.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0a" su ciascun nodo e il traffico del cluster continua attraverso lo switch e la porta "e0b" su ciascun nodo:



b. Collegare le porte del gruppo 1 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2:



3. L'opzione di rete cluster senza switch passa da `false` A `true` . L'operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione senza interruttore sia impostata su `true` :

```
network options switchless-cluster show
```

L'esempio seguente mostra che il cluster switchless è abilitato:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)

```



Prima di procedere al passaggio successivo, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

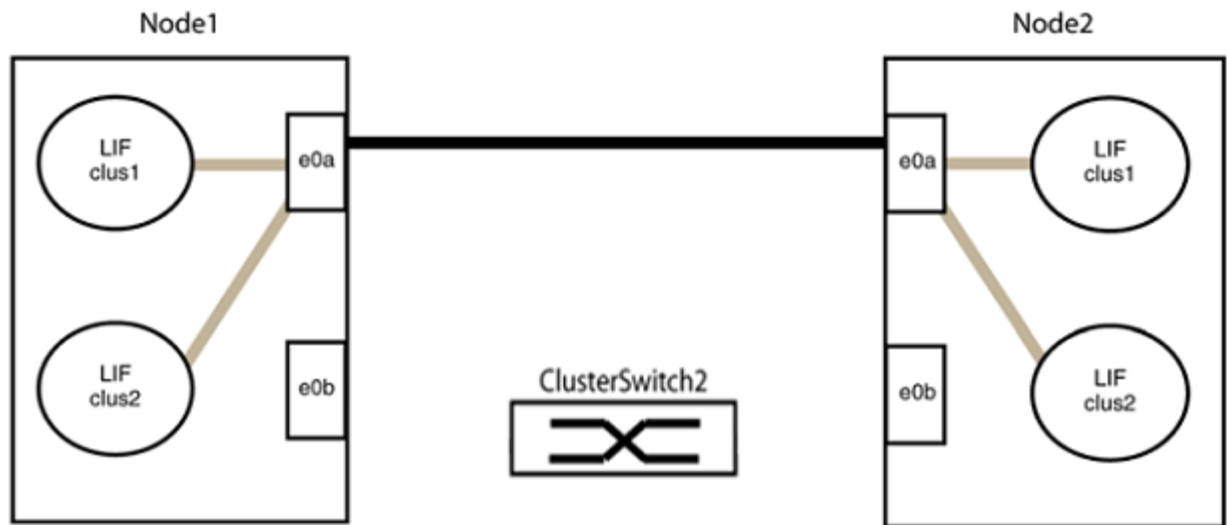
1. Impostare la configurazione senza switch per le porte nel gruppo 2.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 2.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua tramite la connessione diretta tra le porte "e0a":



b. Cablare le porte del gruppo 2 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2 e "e0b" sul nodo 1 è connesso a "e0b" sul nodo 2:



Passaggio 3: verificare la configurazione

1. Verificare che le porte su entrambi i nodi siano collegate correttamente:

```
network device-discovery show -port cluster_port
```

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono correttamente collegate alla porta corrispondente sul partner del cluster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a    node2                      e0a        AFF-A300
           e0b    node2                      e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                      e0a        AFF-A300
           e0b    node1                      e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Riattivare il ripristino automatico per i LIF del cluster:

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

3. Verificare che tutti i LIF siano a casa. Potrebbero volerci alcuni secondi.

```
network interface show -vserver Cluster -lif lif_name
```

Mostra esempio

I LIF sono stati ripristinati se la colonna "È a casa" è true , come mostrato per node1_clus2 E node2_clus2 nell'esempio seguente:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Se uno qualsiasi dei LIFS del cluster non è tornato alle proprie porte home, ripristinarlo manualmente dal nodo locale:

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

4. Controllare lo stato del cluster dei nodi dalla console di sistema di uno dei due nodi:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra epsilon su entrambi i nodi da false :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Per maggiori informazioni, vedere ["Articolo 1010449 della Knowledge Base NetApp : Come sopprimere la creazione automatica di casi durante le finestre di manutenzione programmata"](#).

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

Cosa succederà ora?

Dopo aver sostituito gli interruttori, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Cisco Nexus 9336C-FX2 o 9336C-FX2-T

Iniziare

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

Gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T fanno parte della piattaforma Cisco Nexus 9000 e possono essere installati in un cabinet di sistema NetApp . Gli switch cluster consentono di creare cluster ONTAP con più di due nodi.

Cisco Nexus 9336C-FX2 (36 porte) è uno switch cluster/storage/dati ad alta densità di porte. Cisco Nexus 9336C-FX2-T (12 porte) è uno switch ad alte prestazioni e bassa densità di porte che supporta configurazioni cluster 10/25/40/100GbE.

Seguire questi passaggi del flusso di lavoro per installare e configurare gli switch Cisco 9336C-FX2 e 9336C-FX2-T.

1

"Rivedere i requisiti di configurazione"

Esaminare i requisiti di configurazione per gli switch cluster 9336C-FX2 e 9336C-FX2-T.

2

"Rivedere i componenti e i numeri delle parti"

Esaminare i componenti e i codici articolo degli switch cluster 9336C-FX2 e 9336C-FX2-T.

3

"Esaminare la documentazione richiesta"

Consultare la documentazione specifica dello switch e del controller per configurare gli switch 9336C-FX2 e 9336C-FX2-T e il cluster ONTAP .

4

"Esaminare i requisiti di Smart Call Home"

Esaminare i requisiti per la funzionalità Cisco Smart Call Home, utilizzata per monitorare i componenti hardware e software della rete.

5

"Installare l'hardware"

Installare l'hardware dello switch.

6

"Configurare il software"

Configurare il software dello switch.

Requisiti di configurazione per gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per l'installazione e la manutenzione degli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T, assicurarsi di rivedere la configurazione e i requisiti di rete.

Supporto ONTAP

ONTAP 9.9.1 e versioni successive

A partire da ONTAP 9.9.1, è possibile utilizzare gli switch Cisco Nexus 9336C-FX2 per combinare funzionalità di storage e cluster in una configurazione di switch condivisa.

Se si desidera creare cluster ONTAP con più di due nodi, sono necessari due switch di rete supportati.



Il monitoraggio dello stato dello switch Ethernet non supporta ONTAP 9.13.1P8 e versioni precedenti e 9.14.1P3 e versioni precedenti o NX-OS versione 10.3(4a)(M).

ONTAP 9.10.1 e versioni successive

Inoltre, a partire da ONTAP 9.10.1, è possibile utilizzare gli switch Cisco Nexus 9336C-FX2-T per combinare funzionalità di storage e cluster in una configurazione di switch condivisa.

Se si desidera creare cluster ONTAP con più di due nodi, sono necessari due switch di rete supportati.

Requisiti di configurazione

Assicurarsi che:

- Hai il numero e il tipo di cavi e connettori per i tuoi switch appropriati. Vedi il ["Hardware Universe"](#) .
- A seconda del tipo di switch che si sta configurando inizialmente, è necessario collegarsi alla porta della console dello switch tramite il cavo della console incluso.

Requisiti di rete

Per tutte le configurazioni dello switch sono necessarie le seguenti informazioni di rete.

- Subnet IP per il traffico di rete di gestione
- Nomi host e indirizzi IP per ciascuno dei controller del sistema di archiviazione e tutti gli switch applicabili
- La maggior parte dei controller dei sistemi di storage vengono gestiti tramite l'interfaccia e0M, collegandosi alla porta di servizio Ethernet (icona a forma di chiave inglese). Nei sistemi AFF A800 e AFF A700s , l'interfaccia e0M utilizza una porta Ethernet dedicata.
- Fare riferimento al ["Hardware Universe"](#) per le ultime informazioni.

Per maggiori informazioni sulla configurazione iniziale dello switch, consultare la seguente guida: ["Guida all'installazione e all'aggiornamento Cisco Nexus 9336C-FX2"](#) .

Cosa c'è dopo?

Dopo aver esaminato i requisiti di configurazione, puoi confermare il tuo ["componenti e numeri di parte"](#).

Componenti e numeri di parte per gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per l'installazione e la manutenzione degli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T, assicurarsi di consultare l'elenco dei componenti e i codici articolo.

Dettagli del numero di parte

Nella tabella seguente sono elencati i codici prodotto e la descrizione degli switch, delle ventole e degli alimentatori 9336C-FX2 e 9336C-FX2-T:

Numero di parte	Descrizione
X190200-CS-PE	Interruttore a grappolo, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Interruttore a grappolo, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Interruttore a grappolo, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G
X190212-CS-PI	Interruttore a grappolo, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	SW, licenza Cisco 9336CFX2 POD a 24 porte
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Kit accessori X190001/X190003
X-NXA-PAC-1100W-PE2	Alimentatore N9K-9336C AC 1100W - Flusso d'aria di scarico lato sinistro
X-NXA-PAC-1100W-PI2	Alimentatore CA N9K-9336C da 1100 W - Flusso d'aria di aspirazione lato sinistro
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flusso d'aria di scarico lato babordo
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flusso d'aria di aspirazione lato sinistro

Licenze Cisco Smart solo per porte 9336C-FX2-T

Per attivare più di 12 porte sullo switch cluster Cisco Nexus 9336C-FX-T, è necessario acquistare una licenza Cisco Smart. Le licenze Cisco Smart vengono gestite tramite gli account Cisco Smart.

1. Se necessario, crea un nuovo account Smart. Vedere ["Crea un nuovo account Smart"](#) per i dettagli.
2. Richiedi l'accesso a un account Smart esistente. Vedere ["Richiedi l'accesso a un account Smart esistente"](#) per i dettagli.



Dopo aver acquistato la licenza Smart, installa l'RCF appropriato per abilitare e configurare tutte le 36 porte disponibili per l'uso.

Cosa c'è dopo?

Dopo aver confermato i componenti e i numeri di parte, puoi rivedere il ["documentazione richiesta"](#).

Requisiti di documentazione per gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per l'installazione e la manutenzione degli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-

T, assicurarsi di consultare la documentazione specifica dello switch e del controller per configurare gli switch Cisco 9336-FX2 e il cluster ONTAP .

Documentazione dello switch

Per configurare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T, è necessaria la seguente documentazione dal "[Supporto per gli switch Cisco Nexus serie 9000](#)" pagina:

Titolo del documento	Descrizione
<i>Guida all'installazione dell'hardware della serie Nexus 9000</i>	Fornisce informazioni dettagliate sui requisiti del sito, dettagli sull'hardware dello switch e opzioni di installazione.
<i>Guide alla configurazione del software dello switch Cisco Nexus serie 9000 (scegli la guida per la versione NX-OS installata sugli switch)</i>	Fornisce le informazioni di configurazione iniziale dello switch necessarie prima di poterlo configurare per il funzionamento ONTAP .
<i>Guida all'aggiornamento e al downgrade del software Cisco Nexus serie NX-OS (scegli la guida per la versione NX-OS installata sui tuoi switch)</i>	Fornisce informazioni su come effettuare il downgrade dello switch al software dello switch supportato ONTAP , se necessario.
<i>Indice principale di riferimento dei comandi NX-OS della serie Cisco Nexus 9000</i>	Fornisce collegamenti ai vari riferimenti ai comandi forniti da Cisco.
<i>Riferimento MIB Cisco Nexus 9000</i>	Descrive i file MIB (Management Information Base) per gli switch Nexus 9000.
<i>Riferimento ai messaggi di sistema NX-OS della serie Nexus 9000</i>	Descrive i messaggi di sistema per gli switch Cisco Nexus serie 9000, quelli informativi e altri che potrebbero aiutare a diagnosticare problemi con i collegamenti, l'hardware interno o il software di sistema.
<i>Note sulla versione NX-OS della serie Cisco Nexus 9000 (selezionare le note per la versione NX-OS installata sugli switch)</i>	Descrive le funzionalità, i bug e le limitazioni della serie Cisco Nexus 9000.
Conformità normativa e informazioni sulla sicurezza per Cisco Nexus serie 9000	Fornisce informazioni sulla conformità alle agenzie internazionali, sulla sicurezza e sugli statuti per gli switch della serie Nexus 9000.

Documentazione dei sistemi ONTAP

Per configurare un sistema ONTAP , sono necessari i seguenti documenti per la versione del sistema operativo da "[ONTAP 9](#)" .

Nome	Descrizione
Istruzioni di installazione e configurazione specifiche del controller	Descrive come installare l'hardware NetApp .
Documentazione ONTAP	Fornisce informazioni dettagliate su tutti gli aspetti delle versioni ONTAP .
"Hardware Universe"	Fornisce informazioni sulla configurazione hardware e sulla compatibilità NetApp .

Documentazione del kit ferroviario e dell'armadio

Per installare uno switch Cisco 9336-FX2 in un cabinet NetApp , consultare la seguente documentazione hardware.

Nome	Descrizione
"Armadio di sistema 42U, guida profonda"	Descrive le FRU associate al cabinet del sistema 42U e fornisce istruzioni per la manutenzione e la sostituzione delle FRU.
"Installare uno switch Cisco 9336-FX2 in un cabinet NetApp"	Descrive come installare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T in un cabinet NetApp a quattro montanti.

Requisiti di Smart Call Home

Per utilizzare Smart Call Home, è necessario configurare uno switch di rete cluster per comunicare tramite e-mail con il sistema Smart Call Home. Inoltre, è possibile configurare facoltativamente lo switch di rete del cluster per sfruttare la funzionalità di supporto Smart Call Home integrata di Cisco.

Smart Call Home monitora i componenti hardware e software della tua rete. Quando si verifica una configurazione critica del sistema, viene generata una notifica tramite e-mail e viene inviato un avviso a tutti i destinatari configurati nel profilo di destinazione.

Smart Call Home monitora i componenti hardware e software della tua rete. Quando si verifica una configurazione critica del sistema, viene generata una notifica tramite e-mail e viene inviato un avviso a tutti i destinatari configurati nel profilo di destinazione.

Prima di poter utilizzare Smart Call Home, è necessario tenere presente i seguenti requisiti:

- Deve essere presente un server di posta elettronica.
- Lo switch deve disporre di connettività IP al server di posta elettronica.
- È necessario configurare il nome del contatto (contatto del server SNMP), il numero di telefono e le informazioni sull'indirizzo. Ciò è necessario per determinare l'origine dei messaggi ricevuti.
- Un ID CCO deve essere associato a un contratto di servizio Cisco SMARTnet appropriato per la tua azienda.
- Per registrare il dispositivo, è necessario che sia attivo il servizio Cisco SMARTnet.

IL ["Sito di supporto Cisco"](#) contiene informazioni sui comandi per configurare Smart Call Home.

Installare l'hardware

Flusso di lavoro di installazione hardware per gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per installare e configurare l'hardware per gli switch cluster 9336C-FX2 e 9336C-FX2-T, attenersi alla seguente procedura:

1

"Completa il foglio di lavoro sul cablaggio"

Il foglio di lavoro di cablaggio di esempio fornisce esempi di assegnazioni di porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che puoi utilizzare per configurare il tuo cluster.

2

"Installare l'interruttore"

Installare gli switch 9336C-FX2 e 9336C-FX2-T.

3

"Installare lo switch in un cabinet NetApp"

Installare gli switch 9336C-FX2 e 9336C-FX2-T e il pannello pass-through in un cabinet NetApp , secondo necessità.

4

"Rivedere il cablaggio e la configurazione"

Esaminare il supporto per le porte Ethernet NVIDIA , i requisiti FEC 25GbE e le informazioni sulle risorse TCAM.

Completare il foglio di lavoro sul cablaggio Cisco Nexus 9336C-FX2 o 9336C-FX2-T

Se desideri documentare le piattaforme supportate, scarica un PDF da questa pagina e compila il foglio di lavoro sul cablaggio.

Il foglio di lavoro di cablaggio di esempio fornisce esempi di assegnazioni di porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che puoi utilizzare per configurare il tuo cluster.

- [Foglio di lavoro di esempio per il cablaggio 9336C-FX2](#)
- [Foglio di lavoro per il cablaggio vuoto 9336C-FX2](#)
- [Foglio di lavoro di cablaggio di esempio 9336C-FX2-T \(12 porte\)](#)
- [Foglio di lavoro per il cablaggio vuoto 9336C-FX2-T \(12 porte\)](#)

Foglio di lavoro di esempio per il cablaggio 9336C-FX2

La definizione di porta di esempio su ciascuna coppia di switch è la seguente:

Interruttore del cluster A		Interruttore del cluster B	
Porta di commutazione	Utilizzo di nodi e porte	Porta di commutazione	Utilizzo di nodi e porte

Interruttore del cluster A		Interruttore del cluster B	
1	Nodo 1 4x10GbE	1	Nodo 1 4x10GbE
2	Nodo 2 4x10GbE	2	Nodo 2 4x10GbE
3	Nodo 4x10GbE 3	3	Nodo 4x10GbE 3
4	Nodo 4x25GbE 4	4	Nodo 4x25GbE 4
5	Nodo 4x25GbE 5	5	Nodo 4x25GbE 5
6	Nodo 4x25GbE 6	6	Nodo 4x25GbE 6
7	Nodo 7 40/100GbE	7	Nodo 7 40/100GbE
8	Nodo 8 40/100GbE	8	Nodo 8 40/100GbE
9	Nodo 9 40/100GbE	9	Nodo 9 40/100GbE
10	Nodo 40/100GbE 10	10	Nodo 40/100GbE 10
11	Nodo 11 40/100GbE	11	Nodo 11 40/100GbE
12	Nodo 40/100GbE 12	12	Nodo 40/100GbE 12
13	Nodo 40/100GbE 13	13	Nodo 40/100GbE 13
14	Nodo 40/100GbE 14	14	Nodo 40/100GbE 14
15	Nodo 40/100GbE 15	15	Nodo 40/100GbE 15
16	Nodo 40/100GbE 16	16	Nodo 40/100GbE 16
17	Nodo 40/100GbE 17	17	Nodo 40/100GbE 17
18	Nodo 40/100GbE 18	18	Nodo 40/100GbE 18
19	Nodo 40/100GbE 19	19	Nodo 40/100GbE 19
20	Nodo 40/100GbE 20	20	Nodo 40/100GbE 20
21	Nodo 21 40/100GbE	21	Nodo 21 40/100GbE
22	Nodo 22 40/100GbE	22	Nodo 22 40/100GbE

Interruttore del cluster A		Interruttore del cluster B	
23	Nodo 40/100GbE 23	23	Nodo 40/100GbE 23
24	Nodo 40/100GbE 24	24	Nodo 40/100GbE 24
25-34	Prenotato	25-34	Prenotato
35	100GbE ISL per commutare la porta B 35	35	100GbE ISL per commutare la porta A 35
36	100GbE ISL per commutare la porta B 36	36	100GbE ISL per commutare la porta A 36

Foglio di lavoro per il cablaggio vuoto 9336C-FX2

È possibile utilizzare il foglio di lavoro di cablaggio vuoto per documentare le piattaforme supportate come nodi in un cluster. La sezione *Connessioni cluster supportate* del "[Hardware Universe](#)" definisce le porte del cluster utilizzate dalla piattaforma.

Interruttore del cluster A		Interruttore del cluster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	

Interruttore del cluster A		Interruttore del cluster B	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25-34	Prenotato	25-34	Prenotato
35	100GbE ISL per commutare la porta B 35	35	100GbE ISL per commutare la porta A 35
36	100GbE ISL per commutare la porta B 36	36	100GbE ISL per commutare la porta A 36

Foglio di lavoro di cablaggio di esempio 9336C-FX2-T (12 porte)

La definizione di porta di esempio su ciascuna coppia di switch è la seguente:

Interruttore del cluster A		Interruttore del cluster B	
Porta di commutazione	Utilizzo di nodi e porte	Porta di commutazione	Utilizzo di nodi e porte
1	Nodo 1 4x10GbE	1	Nodo 1 4x10GbE
2	Nodo 2 4x10GbE	2	Nodo 2 4x10GbE
3	Nodo 4x10GbE 3	3	Nodo 4x10GbE 3

Interruttore del cluster A		Interruttore del cluster B	
4	Nodo 4x25GbE 4	4	Nodo 4x25GbE 4
5	Nodo 4x25GbE 5	5	Nodo 4x25GbE 5
6	Nodo 4x25GbE 6	6	Nodo 4x25GbE 6
7	Nodo 7 40/100GbE	7	Nodo 7 40/100GbE
8	Nodo 8 40/100GbE	8	Nodo 8 40/100GbE
9	Nodo 9 40/100GbE	9	Nodo 9 40/100GbE
10	Nodo 40/100GbE 10	10	Nodo 40/100GbE 10
dall'11 al 34	Richiede licenza	dall'11 al 34	Richiede licenza
35	100GbE ISL per commutare la porta B 35	35	100GbE ISL per commutare la porta A 35
36	100GbE ISL per commutare la porta B 36	36	100GbE ISL per commutare la porta A 36

Foglio di lavoro per il cablaggio vuoto 9336C-FX2-T (12 porte)

È possibile utilizzare il foglio di lavoro di cablaggio vuoto per documentare le piattaforme supportate come nodi in un cluster. La sezione *Connessioni cluster supportate* del "[Hardware Universe](#)" definisce le porte del cluster utilizzate dalla piattaforma.

Interruttore del cluster A		Interruttore del cluster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	

Interruttore del cluster A		Interruttore del cluster B	
8		8	
9		9	
10		10	
dall'11 al 34	Richiede licenza	dall'11 al 34	Richiede licenza
35	100GbE ISL per commutare la porta B 35	35	100GbE ISL per commutare la porta A 35
36	100GbE ISL per commutare la porta B 36	36	100GbE ISL per commutare la porta A 36

Vedi il ["Hardware Universe"](#) per maggiori informazioni sulle porte dello switch.

Cosa c'è dopo?

Dopo aver completato i fogli di lavoro sui cavi, puoi ["installare l'interruttore"](#).

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

Seguire questa procedura per impostare e 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 ["Download del 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. Installare gli switch e i controller della rete del cluster e della rete di gestione.

Se stai installando...	Poi...
Cisco Nexus 9336C-FX2 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 9336C-FX2 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 i fogli di lavoro di cablaggio compilati.
3. Accendere la rete del cluster e gli switch e i controller della rete di gestione.

Cosa succederà ora?

Facoltativamente, puoi ["installare uno switch Cisco Nexus 9336C-FX2 in un cabinet NetApp"](#). Altrimenti vai a ["rivedere il cablaggio e la configurazione"](#).

Installare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T in un cabinet NetApp

A seconda della configurazione, potrebbe essere necessario installare lo switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T e il pannello pass-through in un cabinet NetApp . Le staffe standard sono incluse con l'interruttore.

Prima di iniziare

Assicurati di avere quanto segue:

- Il kit del pannello passante è disponibile presso NetApp (codice articolo X8784-R6).

Il kit del pannello pass-through NetApp contiene il seguente hardware:

- Un pannello cieco passante
- Quattro viti 10-32 x .75
- Quattro dadi a clip 10-32
- Per ogni switch, otto viti 10-32 o 12-24 e dadi a clip per montare le staffe e le guide scorrevoli sui montanti anteriori e posteriori del mobile.
- Kit di guide standard Cisco per installare lo switch in un cabinet NetApp .



I cavi di collegamento non sono inclusi nel kit pass-through e dovrebbero essere inclusi con gli switch. Se non sono stati spediti con gli switch, è possibile ordinarli da NetApp (codice articolo X1558A-R6).

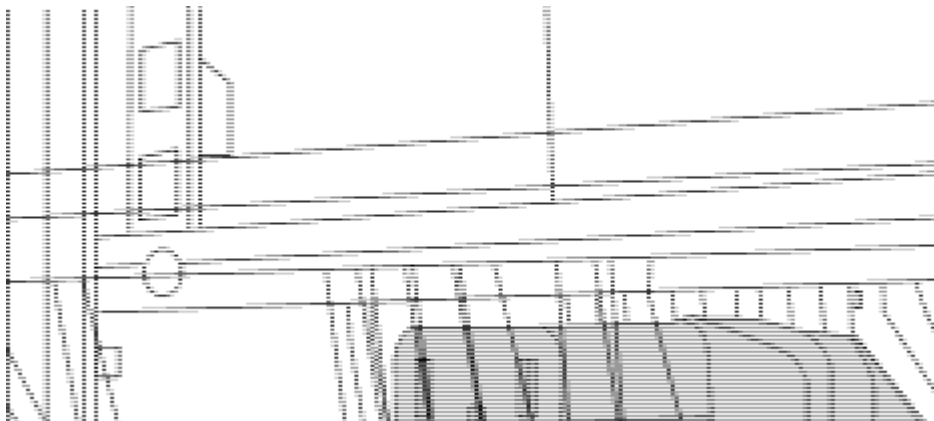
- Per i requisiti di preparazione iniziale, il contenuto del kit e le precauzioni di sicurezza, vedere ["Guida all'installazione dell'hardware Cisco Nexus serie 9000"](#) .

Passi

1. Installare il pannello cieco passante nell'armadio NetApp .
 - a. Determinare la posizione verticale degli interruttori e del pannello cieco nell'armadio.

In questa procedura, il pannello cieco viene installato in U40.

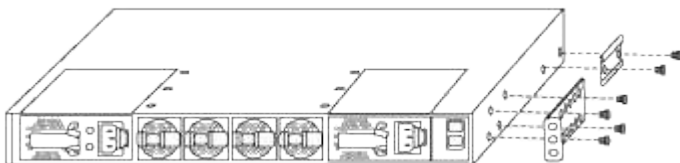
- b. Installare due dadi a clip su ciascun lato nei fori quadrati appropriati per le guide anteriori del mobile.
- c. Centrare il pannello verticalmente per evitare intrusioni nello spazio rack adiacente, quindi serrare le viti.
- d. Inserire i connettori femmina di entrambi i cavi jumper da 48 pollici dalla parte posteriore del pannello e attraverso il gruppo spazzole.



(1) *Connettore femmina del cavo di collegamento.*

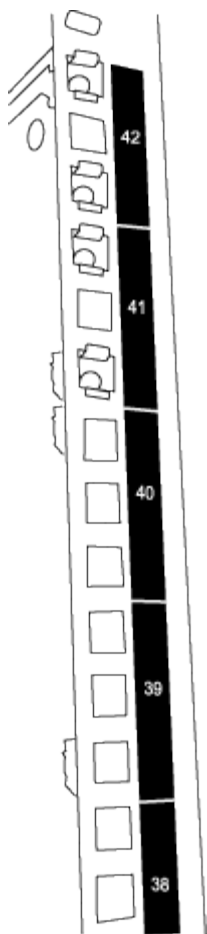
2. Installare le staffe di montaggio su rack sullo chassis dello switch Nexus 9336C-FX2.

- a. Posizionare una staffa di montaggio su rack anteriore su un lato del telaio dello switch in modo che l'aletta di montaggio sia allineata con la piastra frontale del telaio (sul lato dell'alimentatore o della ventola), quindi utilizzare quattro viti M4 per fissare la staffa al telaio.



- b. Ripetere il passaggio 2a con l'altra staffa di montaggio su rack anteriore sull'altro lato dello switch.
- c. Installare la staffa di montaggio posteriore sul telaio dello switch.
- d. Ripetere il passaggio 2c con l'altra staffa di montaggio su rack posteriore sull'altro lato dello switch.

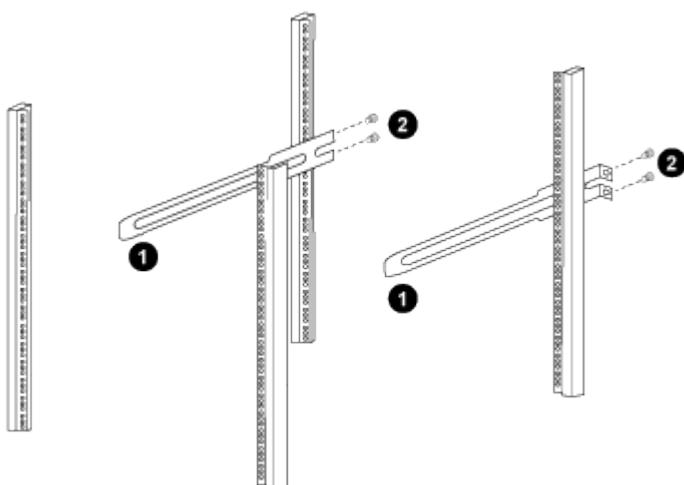
3. Installare i dadi a clip nelle posizioni dei fori quadrati per tutti e quattro i pali IEA.



I due switch 9336C-FX2 e 9336C-FX2-T sono sempre montati nella parte superiore 2U del cabinet RU41 e 42.

4. Installare le guide scorrevoli nel mobile.

- a. Posizionare la prima guida scorrevole sul segno RU42 sul lato posteriore del montante posteriore sinistro, inserire le viti con il tipo di filettatura corrispondente e quindi serrare le viti con le dita.



(1) Mentre fai scorrere delicatamente la guida scorrevole, allineala ai fori delle viti nel rack.

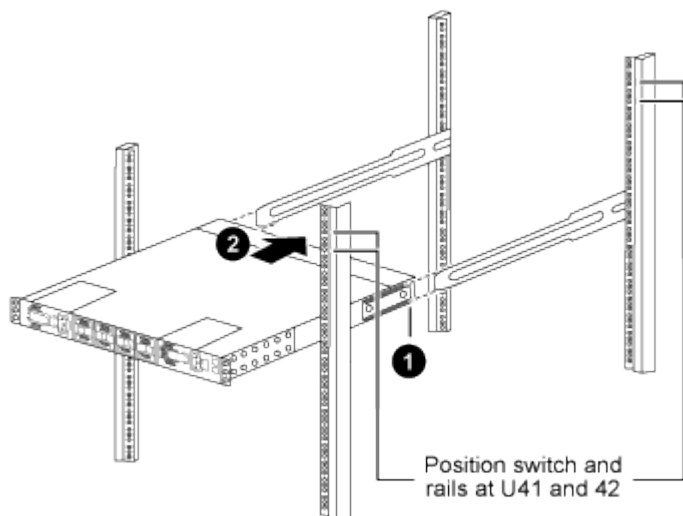
(2) Serrare le viti delle guide scorrevoli ai montanti del mobile.

- a. Ripetere il passaggio 4a per il montante posteriore destro.
 - b. Ripetere i passaggi 4a e 4b nelle posizioni RU41 sull'armadio.
5. Installare l'interruttore nell'armadio.



Per questa operazione sono necessarie due persone: una persona sostiene l'interruttore dalla parte anteriore e un'altra lo guida nelle guide scorrevoli posteriori.

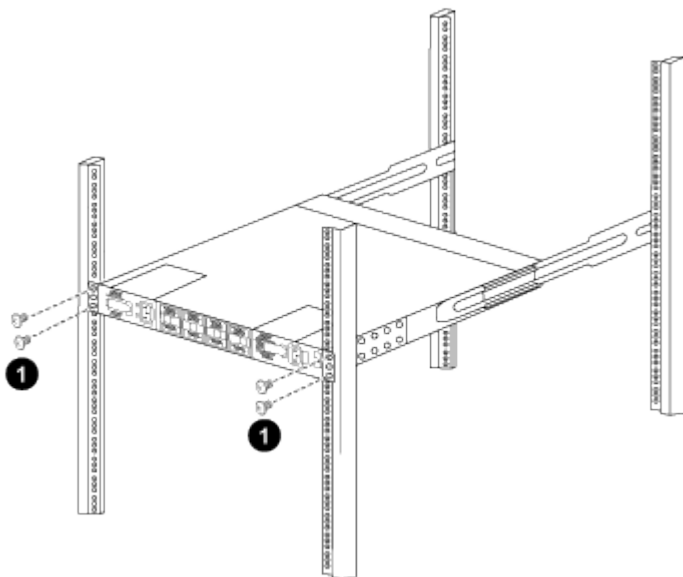
- a. Posizionare la parte posteriore dell'interruttore su RU41.



(1) Mentre il telaio viene spinto verso i montanti posteriori, allineare le due guide di montaggio posteriori del rack con le guide scorrevoli.

(2) Far scorrere delicatamente l'interruttore finché le staffe di montaggio sul rack anteriore non sono a filo con i montanti anteriori.

- b. Fissare l'interruttore all'armadietto.



(1) Mentre una persona tiene in piano la parte anteriore del telaio, l'altra persona deve stringere completamente le quattro viti posteriori ai montanti del mobile.

- a. Ora che il telaio è supportato senza assistenza, serrare completamente le viti anteriori ai montanti.
- b. Ripetere i passaggi da 5a a 5c per il secondo interruttore nella posizione RU42.



Utilizzando come supporto l'interruttore completamente installato, non è necessario tenere ferma la parte anteriore del secondo interruttore durante il processo di installazione.

6. Una volta installati gli interruttori, collegare i cavi di collegamento alle prese di alimentazione degli interruttori.
7. Collegare le spine maschio di entrambi i cavi di collegamento alle prese PDU più vicine disponibili.



Per mantenere la ridondanza, i due cavi devono essere collegati a PDU diverse.

8. Collegare la porta di gestione su ogni switch 9336C-FX2 e 9336C-FX2-T a uno degli switch di gestione (se ordinati) oppure collegarli direttamente alla rete di gestione.

La porta di gestione è la porta in alto a destra situata sul lato PSU dello switch. Dopo l'installazione degli switch, il cavo CAT6 di ogni switch deve essere instradato attraverso il pannello passante per connettersi agli switch di gestione o alla rete di gestione.

Cosa succederà ora?

Dopo aver installato gli switch nell'armadio NetApp, è possibile [configurare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T](#).

Esaminare le considerazioni sul cablaggio e sulla configurazione

Prima di configurare gli switch 9336C-FX2 e 9336C-FX2-T, leggere le seguenti considerazioni.

Supporto per porte Ethernet NVIDIA CX6, CX6-DX e CX7

Se si collega una porta dello switch a un controller ONTAP utilizzando le porte NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7), è necessario codificare la velocità della porta dello switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Vedi il ["Hardware Universe"](#) per maggiori informazioni sulle porte dello switch. 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.

Porte FAS2820 e0a/e0b

Le porte FAS2820 e0a ed e0b richiedono modifiche alla configurazione FEC per collegarsi alle porte dello switch 9336C-FX2 e 9336C-FX2-T. Per le porte dello switch e0a ed e0b, l'impostazione fec è impostata su `rs-cons16`.

```
(cs1)(config)# interface Ethernet1/8-9
(cs1)(config-if-range)# fec rs-cons16
(cs1)(config-if-range)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Le porte non si collegano a causa delle risorse TCAM

Sugli switch 9336C-FX2 e 9336C-FX2-T, le risorse TCAM (Ternary Content Addressable Memory) configurate nella configurazione utilizzata dallo switch sono esaurite.

Vedi l'articolo della Knowledge Base ["Le porte non si collegano su Cisco Nexus 9336C-FX2 a causa delle risorse TCAM"](#) per i dettagli su come risolvere questo problema.

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.

Richiesta	Risposta
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.
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/ras1).	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.

Richiesta	Risposta
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.
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
```

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

```
Node: cluster1-01
```

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

```
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:

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 cluster1-02
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 fare quanto segue:

- Eseguire il `show install all impact nxos bootflash:<image_name>.bin` comando sullo switch per valutare l'impatto dell'installazione o dell'aggiornamento della nuova immagine software NX-OS. Verifica l'integrità dell'immagine, controlla la necessità di riavvii, valuta la compatibilità hardware e conferma la disponibilità di spazio sufficiente.
- Esaminare le note di rilascio per la versione del software NX-OS di destinazione per verificare eventuali requisiti specifici.
- Verificare di disporre di un backup aggiornato della configurazione dello switch.
- Verificare di avere 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
          e0b    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

4. 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 -ipospace 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

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

c. 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
```

```
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 -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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

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

8 entries were displayed.

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

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

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

```

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

2 entries were displayed.

```

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:

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

Se 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
Cluster-HA-Storage RCF 1.xx

Nome RCF
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
Pol	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					
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

						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.

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:

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:

301

```

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.

Migrare gli switch

Migrazione dagli switch cluster NetApp CN1610 agli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T

È possibile migrare gli switch cluster NetApp CN1610 per un cluster ONTAP verso gli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T. Si tratta di una procedura non distruttiva.

Requisiti di revisione

Quando si sostituiscono gli switch cluster NetApp CN1610 con gli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T, è necessario conoscere alcune informazioni sulla configurazione, sulle connessioni delle porte e sui

requisiti di cablaggio. È inoltre necessario verificare il numero di serie dello switch per assicurarsi che venga migrato lo switch corretto.

Switch supportati

Sono supportati i seguenti switch cluster:

- NetApp CN1610
- Cisco 9336C-FX2
- Cisco 9336C-FX2-T

Per i dettagli sulle porte supportate e le relative configurazioni, vedere ["Hardware Universe"](#) . 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.

Cosa ti servirà

Verifica che la tua configurazione soddisfi i seguenti requisiti:

- Il cluster esistente è configurato e funzionante correttamente.
- Tutte le porte del cluster sono nello stato **attivo** per garantire operazioni senza interruzioni.
- Gli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T sono configurati e funzionano con la versione corretta di NX-OS installata con il file di configurazione di riferimento (RCF) applicato.
- La configurazione di rete del cluster esistente è la seguente:
 - Un cluster NetApp ridondante e completamente funzionale che utilizza switch NetApp CN1610.
 - Connettività di gestione e accesso alla console sia per gli switch NetApp CN1610 che per i nuovi switch.
 - Tutti i cluster LIF nello stato attivo con i cluster LIF sulle loro porte home.
- Alcune porte sono configurate sugli switch Cisco 9336C-FX2 e 9336C-FX2-T per funzionare a 40GbE o 100GbE.
- Hai pianificato, migrato e documentato la connettività 40GbE e 100GbE dai nodi agli switch cluster Cisco 9336C-FX2 e 9336C-FX2-T.

Migrare gli switch

Informazioni sugli esempi

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

- Gli switch cluster CN1610 esistenti sono *C1* e *C2*.
- I nuovi switch cluster 9336C-FX2 sono *cs1* e *cs2*.
- I nodi sono *node1* e *node2*.
- I LIF del cluster sono *node1_clus1* e *node1_clus2* sul nodo 1, e *node2_clus1* e *node2_clus2* sul nodo 2, rispettivamente.
- IL `cluster1::*>` il prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono *e3a* e *e3b*.

Informazioni su questo compito

Questa procedura copre il seguente scenario:

- Lo switch C2 viene sostituito prima dallo switch cs2.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Tutti i cluster LIF eseguono il failover sul nuovo switch cs2.
 - Il cablaggio tra i nodi e C2 viene quindi scollegato da C2 e ricollegato a cs2.
- Lo switch C1 è sostituito dallo switch cs1.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Tutti i cluster LIF eseguono il failover sul nuovo switch cs1.
 - Il cablaggio tra i nodi e C1 viene quindi scollegato da C1 e ricollegato a cs1.



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 esegue il failover di tutti i LIF del cluster sullo switch partner operativo, eseguendo al contempo i passaggi sullo switch di destinazione.

Fase 1: Prepararsi alla migrazione

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.

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

3. Disabilitare il ripristino automatico sui LIF del cluster.

Disabilitando il ripristino automatico per questa procedura, i LIF del cluster non torneranno automaticamente alla loro porta home. Rimangono sulla porta attuale finché questa continua a essere attiva e operativa.

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

Passaggio 2: configurare porte e cablaggio

1. Determinare lo stato amministrativo o operativo per ciascuna interfaccia del cluster.

Ogni porta dovrebbe essere visualizzata per `Link E healthy per Health Status`.

- a. Visualizza gli attributi della porta di rete:

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

Mostra esempio

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

b. Visualizza informazioni sui LIF e sui nodi domestici designati:

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

Ogni LIF dovrebbe visualizzare up/up per Status Admin/Oper E true per Is Home .

Mostra esempio

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e3a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e3a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

2. Le porte del cluster su ciascun nodo vengono collegate agli switch del cluster esistenti nel modo seguente (dal punto di vista dei nodi) utilizzando il comando:

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

Mostra esempio

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/1	-
	e3b	C2 (6a:ad:4f:98:4c:a4)	0/1	-
node2	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/2	-
	e3b	C2 (6a:ad:4f:98:4c:a4)	0/2	-

3. Le porte e gli switch del cluster vengono collegati nel modo seguente (dal punto di vista degli switch) utilizzando il comando:

```
show cdp neighbors
```

Mostra esempio



C1# **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 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
C2 0/13	0/13	179	S I s	CN1610
C2 0/14	0/14	175	S I s	CN1610
C2 0/15	0/15	179	S I s	CN1610
C2 0/16	0/16	175	S I s	CN1610

C2# **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 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
C1 0/13	0/13	175	S I s	CN1610
C1 0/14	0/14	175	S I s	CN1610
C1 0/15	0/15	175	S I s	CN1610
C1 0/16	0/16	175	S I s	CN1610

4. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
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. Sullo switch C2, spegnere le porte connesse alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.



Non tentare di migrare manualmente i LIF del cluster.

```

(C2)# configure
(C2)(Config)# interface 0/1-0/12
(C2)(Interface 0/1-0/12)# shutdown
(C2)(Interface 0/1-0/12)# exit
(C2)(Config)# exit

```

2. Spostare le porte del cluster di nodi dal vecchio switch C2 al nuovo switch cs2, utilizzando il cablaggio appropriato supportato da Cisco 9336C-FX2 e 9336C-FX2-T.
3. Visualizza gli attributi della porta di rete:

```
network port show -ipSpace Cluster
```

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node1	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/1	
CN1610				
	e3b	cs2 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
node2	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/2	
CN1610				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				

5. Sullo switch cs2, verificare che tutte le porte del cluster dei nodi siano attive:

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

Mostra esempio

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

Current Is	Logical	Status	Network	Current
Vserver	Interfac	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
	node1_clus1	up/up	169.254.3.4/16	node1
e0b	false			
	node1_clus2	up/up	169.254.3.5/16	node1
e0b	true			
	node2_clus1	up/up	169.254.3.8/16	node2
e0b	false			
	node2_clus2	up/up	169.254.3.9/16	node2
e0b	true			

6. Sullo switch C1, spegnere le porte collegate alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.

```
(C1) # configure
(C1) (Config) # interface 0/1-0/12
(C1) (Interface 0/1-0/12) # shutdown
(C1) (Interface 0/1-0/12) # exit
(C1) (Config) # exit
```

7. Spostare le porte del cluster di nodi dal vecchio switch C1 al nuovo switch cs1, utilizzando il cablaggio appropriato supportato da Cisco 9336C-FX2 e 9336C-FX2-T.
8. Verificare la configurazione finale del cluster:

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

Ogni porta dovrebbe visualizzare up per Link E healthy per Health Status .

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

9. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node1	/cdp			
	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				
node2	/cdp			
	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				

10. Sugli switch cs1 e cs2, verificare che tutte le porte del cluster di nodi siano attive:

```
network port show -ipSpace Cluster
```

Mostra esempio

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

Node: node1

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: node2

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						

11. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

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

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cluster1::*> network device-discovery show -protocol cdp
Node/          Local   Discovered
Protocol       Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1          /cdp
              e0a    cs1 (b8:ce:f6:19:1b:42)   Ethernet1/1/1   N9K-
C9336C-FX2
              e0b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
node2          /cdp
              e0a    cs1 (b8:ce:f6:19:1b:42)   Ethernet1/1/1   N9K-
C9336C-FX2
              e0b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
```

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster:

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

2. Sullo switch cs2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle rispettive porte home.

```
cs2> enable  
cs2# configure  
cs2(config)# interface eth1/1-1/2  
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit  
cs2(config)# exit  
cs2#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home (l'operazione potrebbe richiedere un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verificare che il cluster sia integro:

```
cluster show
```

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
```



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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      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. Riporta il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Migrazione dagli switch Cisco più vecchi agli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T

È possibile eseguire una migrazione senza interruzioni dagli switch cluster Cisco più vecchi agli switch di rete cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Requisiti di revisione

Assicurarsi che:

- Hai verificato il numero di serie dello switch per assicurarti che sia stato migrato lo switch corretto.

- Alcune porte degli switch Nexus 9336C-FX2 sono configurate per funzionare a 10GbE o 40GbE.
- La connettività 10GbE e 40GbE dai nodi agli switch cluster Nexus 9336C-FX2 è stata pianificata, migrata e documentata.
- Il cluster è perfettamente funzionante (non dovrebbero esserci errori nei log o problemi simili).
- La personalizzazione iniziale degli switch Cisco Nexus 9336C-FX2 è completa, in modo che:
 - Gli switch 9336C-FX2 utilizzano la versione software più recente consigliata.
 - Verificare che i file di configurazione di riferimento (RCF) siano stati applicati completamente a tutti i nuovi switch prima di migrare i LIF ai nuovi switch.
 - Controllare le configurazioni di esecuzione e di avvio su entrambi gli switch prima di spostare il traffico di rete.
 - Sui nuovi switch vengono configurate tutte le personalizzazioni del sito, come DNS, NTP, SMTP, SNMP e SSH.
- Hai accesso alla tabella di compatibilità degli switch su ["Switch Ethernet Cisco"](#) pagina per le versioni ONTAP, NX-OS e RCF supportate.
- Hai esaminato le guide software e di aggiornamento appropriate disponibili sul sito Web Cisco per le procedure di aggiornamento e downgrade dello switch Cisco a ["Supporto per gli switch Cisco Nexus serie 9000"](#) pagina.



Se si modifica la velocità delle porte cluster e0a ed e1a sui sistemi AFF A800 o AFF C800 , è possibile che vengano ricevuti pacchetti malformati dopo la conversione della velocità. Vedere ["Errore 1570339"](#) e l'articolo della Knowledge Base ["Errori CRC sulle porte T6 dopo la conversione da 40 GbE a 100 GbE"](#) per una guida.

Migrare gli switch

Informazioni sugli esempi

Gli esempi in questa procedura utilizzano due nodi. Questi nodi utilizzano due porte di interconnessione cluster 10GbE e0a ed e0b. Vedi il ["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.

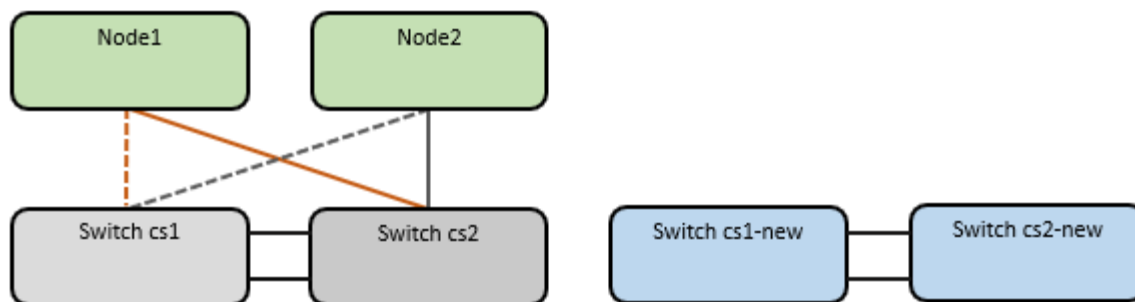


Gli output dei comandi potrebbero variare a seconda delle diverse versioni di ONTAP.

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

- I nomi dei due switch Cisco esistenti sono **cs1** e **cs2**
- I nuovi switch cluster Nexus 9336C-FX2 sono **cs1-new** e **cs2-new**.
- I nomi dei nodi sono **node1** e **node2**.
- I nomi LIF del cluster sono **node1_clus1** e **node1_clus2** per il nodo 1, e **node2_clus1** e **node2_clus2** per il nodo 2.
- Il prompt **cluster1::>** indica il nome del cluster.

Durante questa procedura, fare riferimento al seguente esempio:



Informazioni su questo compito

La procedura richiede l'utilizzo sia dei comandi ONTAP che "Switch serie Nexus 9000" comandi; vengono utilizzati i comandi ONTAP , salvo diversa indicazione.

Questa procedura copre il seguente scenario:

- Lo switch cs2 viene sostituito prima dallo switch cs2-new.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Tutti i cluster LIF eseguono il failover sul nuovo switch cs2-new.
 - Il cablaggio tra i nodi e cs2 viene quindi scollegato da cs2 e ricollegato a cs2-new.
- Lo switch cs1 è sostituito dallo switch cs1-new.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Tutti i LIF del cluster eseguono il failover sul nuovo switch cs1-new.
 - Il cablaggio tra i nodi e cs1 viene quindi scollegato da cs1 e ricollegato a cs1-new.



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 esegue il failover di tutti i LIF del cluster sullo switch partner operativo, eseguendo al contempo i passaggi sullo switch di destinazione.

Fase 1: Prepararsi alla migrazione

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
```

Viene visualizzato il prompt avanzato (*>).

Passaggio 2: configurare porte e cablaggio

1. Sui nuovi switch, verificare che l'ISL sia cablato e funzionante tra gli switch cs1-new e cs2-new:

```
show port-channel summary
```

Mostra esempio

```
cs1-new# 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)

cs2-new# 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)
```

2. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster esistenti:

```
network device-discovery show
```

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1      /cdp
           e0a    cs1                      Ethernet1/1    N5K-
C5596UP
           e0b    cs2                      Ethernet1/2    N5K-
C5596UP
node2      /cdp
           e0a    cs1                      Ethernet1/1    N5K-
C5596UP
           e0b    cs2                      Ethernet1/2    N5K-
C5596UP
```

3. Determinare lo stato amministrativo o operativo di ogni porta del cluster.

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

```
network port show -ipospace Cluster
```

Mostra esempio

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

Node: node1

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					

Node: node2

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					

b. Verificare che tutte le interfacce cluster (LIF) siano sulle rispettive porte home:

```
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				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
e0b	node1_clus2	up/up	169.254.49.125/16	node1
e0a	node2_clus1	up/up	169.254.47.194/16	node2
e0b	node2_clus2	up/up	169.254.19.183/16	node2

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 Model	Type	Address	
-----	-----	-----	
cs1 C5596UP	cluster-network	10.233.205.92	N5K-
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 C5596UP	cluster-network	10.233.205.93	N5K-
Serial Number: FOXXXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version			
9.3(4)			
Version Source: CDP			

4. Disabilitare il ripristino automatico sui LIF del cluster.

Disabilitando il ripristino automatico per questa procedura, i LIF del cluster non torneranno automaticamente alla loro porta home. Rimangono sulla porta attuale finché questa continua a essere attiva e operativa.

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



La disabilitazione del ripristino automatico garantisce che ONTAP esegua il failover sui LIF del cluster solo quando le porte dello switch vengono successivamente arrestate.

5. Sullo switch del cluster cs2, chiudere le porte connesse alle porte del cluster di **tutti** i nodi per eseguire il failover dei LIF del cluster:

```

cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#

```

6. 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				
	node1_clus1	up/up	169.254.3.4/16	node1
e0a	true			
	node1_clus2	up/up	169.254.3.5/16	node1
e0a	false			
	node2_clus1	up/up	169.254.3.8/16	node2
e0a	true			
	node2_clus2	up/up	169.254.3.9/16	node2
e0a	false			

7. Verificare che il cluster sia integro:

```
cluster show
```

Mostra esempio

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

8. Se i LIF del cluster hanno fallito nello switch cs1 e il cluster è integro, andare a [Fare un passo. 10](#) . Se alcuni LIF del cluster non sono integri o il cluster non è integro, è possibile ripristinare la connettività allo switch cs2, come segue:

- a. Visualizza le porte connesse alle porte del cluster di **tutti** i nodi:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# no shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

- b. 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				
	node1_clus1	up/up	169.254.3.4/16	node1
e0a	true			
	node1_clus2	up/up	169.254.3.5/16	node1
e0a	false			
	node2_clus1	up/up	169.254.3.8/16	node2
e0a	true			
	node2_clus2	up/up	169.254.3.9/16	node2
e0a	false			

- c. Verificare che il cluster sia integro:

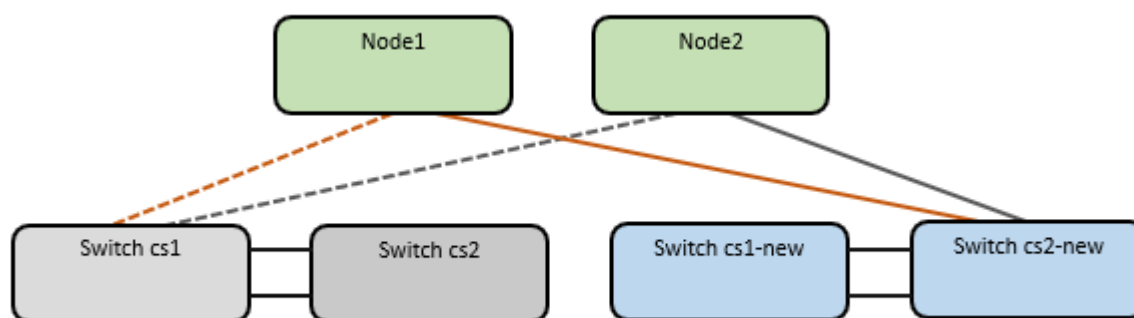
```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node      Health Eligibility Epsilon
-----
node1     true   true      false
node2     true   true      false
```

9. Dopo aver ripristinato LIF e lo stato del cluster, riavviare il processo da [Fare un passo. 4](#).
10. Spostare tutti i cavi di connessione dei nodi del cluster dal vecchio switch cs2 al nuovo switch cs2-new.

I cavi di collegamento del nodo cluster sono stati spostati sullo switch cs2-new



11. Conferma lo stato delle connessioni di rete spostate su cs2-new:

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

Mostra esempio

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

Node: node1

Ignore

						Speed(Mbps)	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: node2

Ignore

						Speed(Mbps)	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						

Tutte le porte del cluster spostate dovrebbero essere attive.

12. Controllare le informazioni sui vicini sulle porte del cluster:

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

Mostra esempio

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform

node1	/cdp			
	e0a	cs1	Ethernet1/1	N5K-
C5596UP				
	e0b	cs2-new	Ethernet1/1/1	N9K-
C9336C-FX2				
node2	/cdp			
	e0a	cs1	Ethernet1/2	N5K-
C5596UP				
	e0b	cs2-new	Ethernet1/1/2	N9K-
C9336C-FX2				

Verificare che le porte del cluster spostate vedano lo switch cs2-new come vicino.

13. Confermare le connessioni delle porte dello switch dal punto di vista dello switch cs2-new:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. Sullo switch del cluster cs1, chiudere le porte connesse alle porte del cluster di **tutti** i nodi per eseguire il failover dei LIF del cluster.

```
cs1# configure
cs1(config)# interface eth1/1-1/2
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
```

Tutti i LIF del cluster eseguono il failover sullo switch cs2-new.

15. Verificare che i LIF del cluster abbiano eseguito il failover sulle porte ospitate sullo switch cs2-new. Potrebbero volerci alcuni secondi:

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

Mostra esempio

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

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

Cluster				
	node1_clus1	up/up	169.254.3.4/16	node1
e0b	false			
	node1_clus2	up/up	169.254.3.5/16	node1
e0b	true			
	node2_clus1	up/up	169.254.3.8/16	node2
e0b	false			
	node2_clus2	up/up	169.254.3.9/16	node2
e0b	true			

16. Verificare che il cluster sia integro:

```
cluster show
```

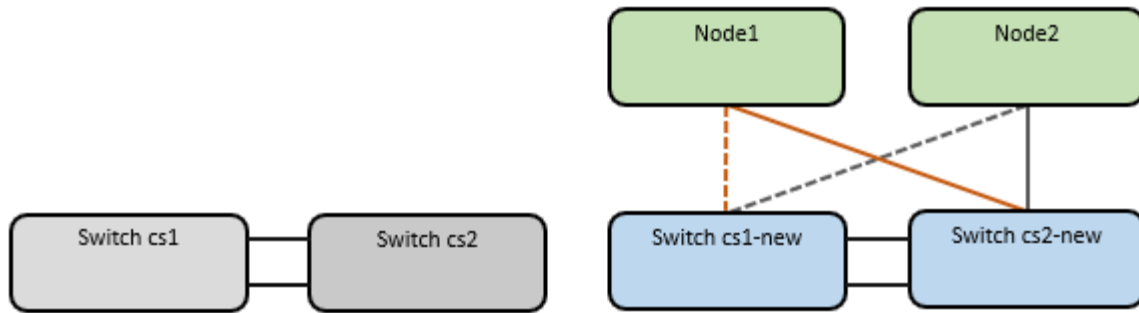
Mostra esempio

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

17. Spostare i cavi di connessione del nodo cluster da cs1 al nuovo switch cs1-new.

I cavi di collegamento del nodo cluster sono stati spostati sullo switch cs1-new



18. Conferma lo stato delle connessioni di rete spostate su cs1-new:

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

Mostra esempio

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Tutte le porte del cluster spostate dovrebbero essere attive.

19. Controllare le informazioni sui vicini sulle porte del cluster:

```
network device-discovery show
```

Mostra esempio

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			

node1	/cdp		
	e0a	cs1-new	Ethernet1/1/1 N9K-
C9336C-FX2			
	e0b	cs2-new	Ethernet1/1/2 N9K-
C9336C-FX2			
node2	/cdp		
	e0a	cs1-new	Ethernet1/1/1 N9K-
C9336C-FX2			
	e0b	cs2-new	Ethernet1/1/2 N9K-
C9336C-FX2			

Verificare che le porte del cluster spostate vedano lo switch cs1-new come vicino.

20. Confermare le connessioni delle porte dello switch dal punto di vista dello switch cs1-new:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

21. Verificare che l'ISL tra cs1-new e cs2-new sia ancora operativo:

```
show port-channel summary
```

Mostra esempio

```
cs1-new# 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)

cs2-new# 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)
```

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster.

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

2. Sullo switch cs2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle rispettive porte home.

```
cs2> enable  
cs2# configure  
cs2(config)# interface eth1/1-1/2  
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit  
cs2(config)# exit  
cs2#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home (l'operazione potrebbe richiedere un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verificare che il cluster sia integro:

```
cluster show
```

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
```



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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      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. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :
`system node autosupport invoke -node * -type all -message MAINT=END`

Cosa succederà ora?

Dopo aver migrato gli switch, puoi [configurare il monitoraggio dello stato dello switch](#) .

Migrare a un cluster commutato a due nodi

Se si dispone di un ambiente cluster a due nodi *senza switch*, è possibile migrare a un ambiente cluster a due nodi *con switch* utilizzando gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T.

Il processo di migrazione funziona per tutti i nodi che utilizzano porte ottiche o Twinax, ma non è supportato su questo switch se i nodi utilizzano porte RJ45 BASE-T da 10 Gb integrate per le porte di rete del cluster.

Requisiti di revisione

Cosa ti servirà

- Per la configurazione switchless a due nodi:
 - La configurazione switchless a due nodi è correttamente configurata e funzionante.

- Tutte le porte del cluster sono nello stato **attivo**.
- Tutte le interfacce logiche del cluster (LIF) sono nello stato **attivo** e sulle loro porte home.
- Vedere ["Hardware Universe"](#) per tutte le versioni ONTAP supportate.
- Per la configurazione dello switch Cisco Nexus 9336C-FX2:
 - Entrambi gli switch dispongono di connettività di rete di gestione.
 - È disponibile l'accesso alla console per gli switch del cluster.
 - Le connessioni da nodo a nodo e da switch a switch del Nexus 9336C-FX2 utilizzano cavi Twinax o in fibra.

Vedere ["Hardware Universe"](#) per maggiori informazioni sul cablaggio.

- I cavi Inter-Switch Link (ISL) sono collegati alle porte 1/35 e 1/36 su entrambi gli switch 9336C-FX2.
- La personalizzazione iniziale di entrambi gli switch 9336C-FX2 è stata completata, in modo che:
 - Gli switch 9336C-FX2 utilizzano la versione software più recente.
 - I file di configurazione di riferimento (RCF) vengono applicati agli switch. Qualsiasi personalizzazione del sito, come SMTP, SNMP e SSH, viene configurata sui nuovi switch.

Informazioni sugli esempi

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

- I nomi degli switch 9336C-FX2 sono cs1 e cs2.
- I nomi degli SVM del cluster sono node1 e node2.
- I nomi dei LIF sono node1_clus1 e node1_clus2 sul nodo 1, e node2_clus1 e node2_clus2 sul nodo 2, rispettivamente.
- IL `cluster1: :*>` il prompt indica il nome del cluster.
- Le porte cluster utilizzate in questa procedura sono e0a ed e0b.

Vedere ["Hardware Universe"](#) per informazioni sulle porte del cluster per le 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.

Migrare gli switch

Fase 1: Prepararsi alla migrazione

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. Cambia il livello di privilegio in avanzato, inserendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato(*>) appare.

Passaggio 2: configurare porte e cablaggio

1. Disabilitare tutte le porte rivolte verso il nodo (non le porte ISL) su entrambi i nuovi switch del cluster cs1 e cs2.

Non disattivare le porte ISL.

Mostra esempio

L'esempio seguente mostra che le porte da 1 a 34 rivolte al nodo sono disabilite sullo switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# shutdown
```

2. Verificare che l'ISL e le porte fisiche sull'ISL tra i due switch 9336C-FX2 cs1 e cs2 siano attivi sulle porte 1/35 e 1/36:

```
show port-channel summary
```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono attive sullo switch cs1:

```
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)
```

L'esempio seguente mostra che le porte ISL sono attive sullo switch cs2:

```
(cs2)# 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)
```

3. Visualizza l'elenco dei dispositivi vicini:

```
show cdp neighbors
```

Questo comando fornisce informazioni sui dispositivi collegati al sistema.

Mostra esempio

L'esempio seguente elenca i dispositivi adiacenti sullo switch cs1:

```
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         Local Intrfce  Hldtme Capability  Platform
Port ID
cs2               Eth1/35       175    R S I s         N9K-C9336C
Eth1/35
cs2               Eth1/36       175    R S I s         N9K-C9336C
Eth1/36

Total entries displayed: 2
```

L'esempio seguente elenca i dispositivi adiacenti sullo switch cs2:

```
cs2# 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         Local Intrfce  Hldtme Capability  Platform
Port ID
cs1               Eth1/35       177    R S I s         N9K-C9336C
Eth1/35
cs1               Eth1/36       177    R S I s         N9K-C9336C
Eth1/36

Total entries displayed: 2
```

4. Verificare che tutte le porte del cluster siano attive:

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

Ogni porta dovrebbe essere visualizzata per Link e sano per Health Status .

Mostra esempio

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

Node: node1

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

Node: node2

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

4 entries were displayed.

5. Verificare che tutti i cluster LIF siano attivi e operativi:

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

Ogni cluster LIF dovrebbe visualizzare true per Is Home e avere un Status Admin/Oper di su/su.

Mostra esempio

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

6. Disabilitare il ripristino automatico su tutti i LIF del cluster:

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

Mostra esempio

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

	Logical	
Vserver	Interface	Auto-revert

Cluster		
	node1_clus1	false
	node1_clus2	false
	node2_clus1	false
	node2_clus2	false

4 entries were displayed.

7. Scollegare il cavo dalla porta e0a del cluster sul nodo 1, quindi collegare e0a alla porta 1 sullo switch cs1 del cluster, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.

IL ["Hardware Universe - Interruttori"](#) contiene maggiori informazioni sul cablaggio.

["Hardware Universe - Interruttori"](#)

8. Scollegare il cavo dalla porta e0a del cluster sul nodo 2, quindi collegare e0a alla porta 2 sullo switch cs1 del cluster, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.
9. Abilitare tutte le porte rivolte verso il nodo sullo switch del cluster cs1.

Mostra esempio

L'esempio seguente mostra che le porte da 1/1 a 1/34 sono abilitate sullo switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# no shutdown
```

10. Verificare che tutti i cluster LIF siano attivi e operativi:

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

Mostra esempio

Il seguente esempio mostra che tutti i LIF sono attivi su node1 e node2:

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
-----	----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0b
false					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0b
false					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.

11. Visualizza informazioni sullo stato dei nodi nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

2 entries were displayed.

12. Scollegare il cavo dalla porta e0b del cluster sul nodo 1, quindi collegare e0b alla porta 1 sullo switch cs2 del cluster, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.
13. Scollegare il cavo dalla porta e0b del cluster sul nodo 2, quindi collegare e0b alla porta 2 sullo switch cs2

del cluster, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.

14. Abilitare tutte le porte rivolte verso il nodo sullo switch cluster cs2.

Mostra esempio

L'esempio seguente mostra che le porte da 1/1 a 1/34 sono abilitate sullo switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs2(config-if-range)# no shutdown
```

15. Verificare che tutte le porte del cluster siano attive:

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

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono attive su node1 e node2:

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

Node: node1

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: node2

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

4 entries were displayed.
```

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster.

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

2. Sullo switch cs2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle rispettive porte home.

```
cs2> enable  
cs2# configure  
cs2(config)# interface eth1/1-1/2  
cs2(config-if-range)# shutdown
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cs2(config-if-range)# no shutdown
```

(After executing the no shutdown command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

```
cs2(config-if-range)# exit  
cs2(config)# exit  
cs2#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home (l'operazione potrebbe richiedere un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

4. Verificare che tutte le interfacce visualizzino true per Is Home :

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



L'operazione potrebbe richiedere diversi minuti.

Mostra esempio

L'esempio seguente mostra che tutti i LIF sono attivi su node1 e node2 e che Is Home i risultati sono veri:

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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.

5. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
show cdp neighbors
```

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
(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
cs2 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs2 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

```
(cs2)# 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 e0b	Eth1/1	133	H	FAS2980
node2 e0b	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

6. Visualizza informazioni sui dispositivi di rete rilevati nel tuo 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
-----
node2      /cdp
           e0a    cs1                      0/2      N9K-
C9336C
           e0b    cs2                      0/2      N9K-
C9336C
node1      /cdp
           e0a    cs1                      0/1      N9K-
C9336C
           e0b    cs2                      0/1      N9K-
C9336C

4 entries were displayed.
```

7. Verificare che le impostazioni siano disabilitate:

```
network options switchless-cluster show
```



Potrebbero essere necessari diversi minuti affinché il comando venga completato. Attendi l'annuncio "Scadenza della durata di 3 minuti".

L'output false nell'esempio seguente mostra che le impostazioni di configurazione sono disabilitate:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

8. Verificare lo stato dei membri del nodo nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

9. 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	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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. Riporta il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituire gli interruttori

Sostituisci gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T

Per sostituire gli switch Nexus 9336C-FX2 e 9336C-FX2-T difettosi in una rete cluster, seguire questi passaggi. Si tratta di una procedura non distruttiva (NDU).

Requisiti di revisione

Prima di procedere alla sostituzione dell'interruttore, accertarsi che:

- Hai verificato il numero di serie dello switch per assicurarti che venga sostituito lo switch corretto.
- Sull'infrastruttura di rete e cluster esistente:
 - Il cluster esistente è stato verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
 - Tutte le porte del cluster sono **attive**.
 - Tutte le interfacce logiche del cluster (LIF) sono **attive** e sulle loro porte home.
 - L'ONTAP `cluster ping-cluster -node node1` il comando deve indicare che la connettività di base e la comunicazione più grande di PMTU hanno esito positivo su tutti i percorsi.
- Sull'interruttore sostitutivo Nexus 9336C-FX2:
 - La connettività della rete di gestione sullo switch sostitutivo è funzionante.
 - L'accesso alla console per l'interruttore sostitutivo è pronto.
 - Le connessioni dei nodi sono le porte da 1/1 a 1/34.
 - Tutte le porte Inter-Switch Link (ISL) sono disabilite sulle porte 1/35 e 1/36.
 - Il file di configurazione di riferimento (RCF) desiderato e l'immagine del sistema operativo NX-OS vengono caricati sullo switch.
 - La personalizzazione iniziale dello switch è completa, come dettagliato in ["Configurare lo switch cluster 9336C-FX2"](#).

Tutte le personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengono copiate sul nuovo switch.

- Hai eseguito il comando per migrare un cluster LIF dal nodo in cui è ospitato il cluster LIF.

Abilita la registrazione della console

NetApp consiglia vivamente di abilitare la registrazione della console sui dispositivi utilizzati e di adottare le seguenti misure quando si sostituisce lo switch:

- Lasciare AutoSupport abilitato durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione di casi per tutta la durata della manutenzione. Vedi questo articolo della Knowledge Base ["SU92: Come sopprimere la creazione automatica dei casi durante le finestre di manutenzione programmata"](#) per ulteriori dettagli.
- Abilita la registrazione delle sessioni per tutte le sessioni CLI. Per istruzioni su come abilitare la registrazione della sessione, consultare la sezione "Registrazione dell'output della sessione" in questo articolo della Knowledge Base ["Come configurare PuTTY per una connettività ottimale ai sistemi ONTAP"](#).

Sostituire l'interruttore

Informazioni sugli esempi

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

- I nomi degli switch Nexus 9336C-FX2 esistenti sono cs1 e cs2.
- Il nome del nuovo switch Nexus 9336C-FX2 è newcs2.
- I nomi dei nodi sono node1 e node2.
- Le porte del cluster su ciascun nodo sono denominate e0a ed e0b.

- I nomi LIF del cluster sono node1_clus1 e node1_clus2 per node1, e node2_clus1 e node2_clus2 per node2.
- Il prompt per le modifiche a tutti i nodi del cluster è cluster1::*>

Informazioni su questo compito

La seguente procedura si basa sulla seguente topologia di rete cluster:

Mostra esempio

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

Node: node1

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: node2

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						

4 entries were displayed.

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	-----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b

```

true
node2_clus1 up/up 169.254.47.194/16 node2 e0a
true
node2_clus2 up/up 169.254.19.183/16 node2 e0b
true
4 entries were displayed.

```

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

```
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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2	Eth1/35	176	R S I s	N9K-C9336C	
Eth1/35					
cs2 (FD0220329V5)	Eth1/36	176	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

```
cs2# 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	Local Intrfce	Hldtme	Capability	Platform	Port
ID					
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1	Eth1/35	178	R S I s	N9K-C9336C	
Eth1/35					
cs1	Eth1/36	178	R S I s	N9K-C9336C	
Eth1/36					

```
Total entries displayed: 4
```

Fase 1: Preparazione alla sostituzione

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. Installare l'RCF e l'immagine appropriati sullo switch, newcs2, ed effettuare tutti i preparativi necessari sul sito.

Se necessario, verificare, scaricare e installare le versioni appropriate del software RCF e NX-OS per il nuovo switch. Se hai verificato che il nuovo switch è configurato correttamente e non necessita di aggiornamenti del software RCF e NX-OS, continua con il passaggio 2.

- a. Accedere alla *Pagina di descrizione del file di configurazione di riferimento degli switch di rete di gestione e cluster NetApp* sul sito di supporto NetApp .
 - b. Fare clic sul collegamento per la *Matrice di compatibilità della rete di cluster e della rete di gestione*, quindi prendere nota della versione del software dello switch richiesta.
 - c. Fai clic sulla freccia indietro del browser per tornare alla pagina Descrizione, fai clic su **CONTINUA**, accetta il contratto di licenza e poi vai alla pagina Download.
 - d. Seguire i passaggi indicati nella pagina Download per scaricare i file RCF e NX-OS corretti per la versione del software ONTAP che si sta installando.
3. Sul nuovo switch, accedi come amministratore e chiudi tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da 1/1 a 1/34).

Se l'interruttore che stai sostituendo non funziona ed è spento, vai al passaggio 4. I LIF sui nodi del cluster dovrebbero già aver eseguito il failover sull'altra porta del cluster per ciascun nodo.

Mostra esempio

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-34
newcs2(config-if-range)# shutdown
```

4. Verificare che tutti i LIF del cluster abbiano il ripristino automatico abilitato:

```
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	node1_clus1	true
Cluster	node1_clus2	true
Cluster	node2_clus1	true
Cluster	node2_clus2	true

4 entries were displayed.

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)

```

Passaggio 2: configurare cavi e porte

1. Disattivare le porte ISL 1/35 e 1/36 sullo switch Nexus 9336C-FX2 cs1.

Mostra esempio

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/35-36
cs1(config-if-range)# shutdown
cs1(config-if-range)#

```

2. Rimuovere tutti i cavi dallo switch Nexus 9336C-FX2 cs2, quindi collegarli alle stesse porte sullo switch Nexus C9336C-FX2 newcs2.
3. Attivare le porte ISL 1/35 e 1/36 tra gli switch cs1 e newcs2, quindi verificare lo stato operativo del canale porta.

Il canale porta deve indicare Po1(SU) e le porte membro devono indicare Eth1/35(P) ed Eth1/36(P).

Mostra esempio

Questo esempio abilita le porte ISL 1/35 e 1/36 e visualizza il riepilogo del canale porta sullo switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/35-36
cs1(config-if-range)# no shutdown

cs1(config-if-range)# 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(config-if-range)#
```

4. Verificare che la porta e0b sia attiva su tutti i nodi:

```
network port show ipspace Cluster
```

Mostra esempio

L'output dovrebbe essere simile al seguente:

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

Node: node1

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

Node: node2

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/auto  -
false

4 entries were displayed.
```

5. Sullo stesso nodo utilizzato nel passaggio precedente, ripristinare il cluster LIF associato alla porta nel passaggio precedente utilizzando il comando `network interface revert`.

Mostra esempio

In questo esempio, LIF node1_clus2 su node1 viene ripristinato correttamente se il valore Home è true e la porta è e0b.

I seguenti comandi restituiscono LIF node1_clus2 SU node1 al porto di casa e0a e visualizza informazioni sui LIF su entrambi i nodi. L'attivazione del primo nodo ha esito positivo se la colonna Is Home è vera per entrambe le interfacce del cluster e mostrano le assegnazioni di porta corrette, in questo esempio e0a E e0b sul nodo 1.

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0a	false			

4 entries were displayed.

6. Visualizza informazioni sui nodi in un cluster:

```
cluster show
```

Mostra esempio

Questo esempio mostra che lo stato di integrità del nodo node1 e node2 in questo cluster è corretto:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	false	true
node2	true	true

7. Verificare che tutte le porte fisiche del cluster siano attive:

```
network port show ipspace Cluster
```

Mostra esempio

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

Node node1
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: node2

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

4 entries were displayed.
```

8. 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	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)
```

Passaggio 3: verificare la configurazione

1. Confermare la seguente configurazione di rete del cluster:

```
network port show
```

Mostra esempio

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

```
Node: node1
```

```
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: node2
```

```
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					

```
4 entries were displayed.
```

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1

```
e0b      true
          node2_clus1  up/up    169.254.47.194/16  node2
e0a      true
          node2_clus2  up/up    169.254.19.183/16  node2
e0b      true
```

4 entries were displayed.

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	0/2	N9K-
C9336C				
	e0b	newcs2	0/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C9336C				
	e0b	newcs2	0/1	N9K-
C9336C				

4 entries were displayed.

```
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	Eth1/1	144	H	FAS2980
e0a				
node2	Eth1/2	145	H	FAS2980
e0a				
newcs2	Eth1/35	176	R S I s	N9K-C9336C
Eth1/35				
newcs2	Eth1/36	176	R S I s	N9K-C9336C

```
Eth1/36
```

```
Total entries displayed: 4
```

```
cs2# 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 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C

```
Total entries displayed: 4
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver sostituito gli interruttori, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituisci gli switch cluster Cisco Nexus 9336C-FX2 e 9336C-FX2-T con connessioni switchless

È possibile migrare da un cluster con una rete di cluster commutata a uno in cui due nodi sono collegati direttamente per ONTAP 9.3 e versioni successive.

Requisiti di revisione

Linee guida

Rivedere le seguenti linee guida:

- La migrazione a una configurazione cluster switchless a due nodi è un'operazione non distruttiva. La maggior parte dei sistemi ha due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per sistemi con un numero maggiore di porte di interconnessione cluster dedicate su ciascun nodo, ad esempio quattro, sei o otto.

- Non è possibile utilizzare la funzionalità di interconnessione del cluster senza switch con più di due nodi.
- Se si dispone di un cluster a due nodi esistente che utilizza switch di interconnessione cluster ed esegue ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

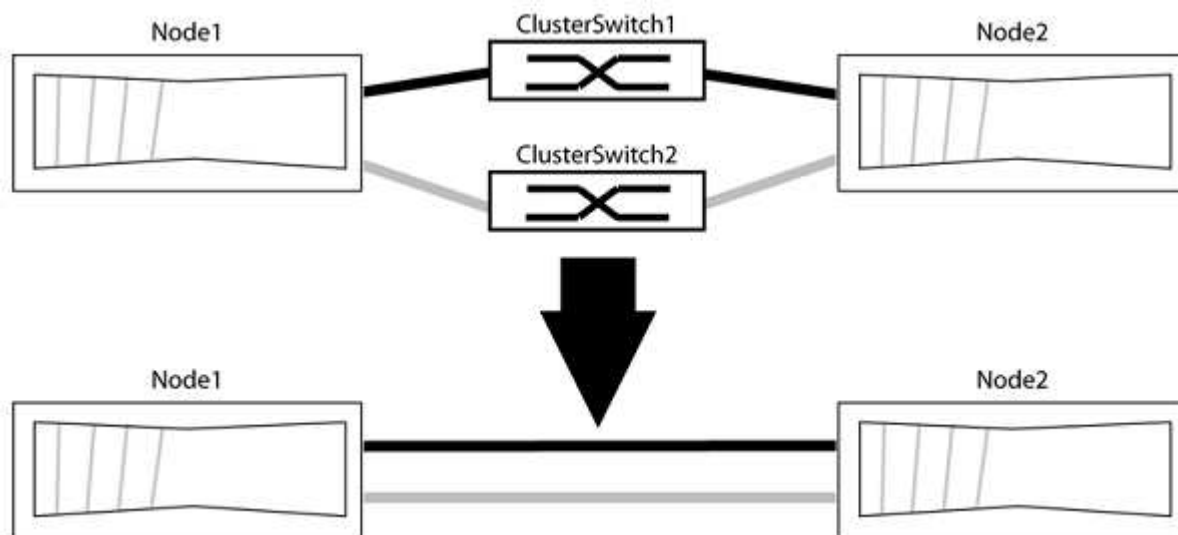
Assicurati di avere quanto segue:

- Un cluster sano costituito da due nodi collegati tramite switch di cluster. I nodi devono eseguire la stessa versione ONTAP .
- Ogni nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, ci sono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

Informazioni su questo compito

La seguente procedura rimuove gli switch del cluster in un cluster a due nodi e sostituisce ogni connessione allo switch con una connessione diretta al nodo partner.



Informazioni sugli esempi

Gli esempi nella seguente procedura mostrano nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse, poiché variano in base al sistema.

Fase 1: Prepararsi alla migrazione

1. Cambia il livello di privilegio in avanzato, inserendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato `*>` appare.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster switchless, abilitato per impostazione predefinita.

È possibile verificare che il rilevamento dei cluster switchless sia abilitato eseguendo il comando con privilegi avanzati:

```
network options detect-switchless-cluster show
```

Mostra esempio

Il seguente output di esempio mostra se l'opzione è abilitata.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Abilita rilevamento cluster senza switch" è `false`, contattare l'assistenza NetApp.

3. 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=<number_of_hours>h
```

Dove `h` è la durata della finestra di manutenzione in ore. Il messaggio avvisa il supporto tecnico di questa attività di manutenzione, in modo che possa sopprimere la creazione automatica dei casi durante la finestra di manutenzione.

Nell'esempio seguente, il comando sopprime la creazione automatica dei casi per due ore:

Mostra esempio

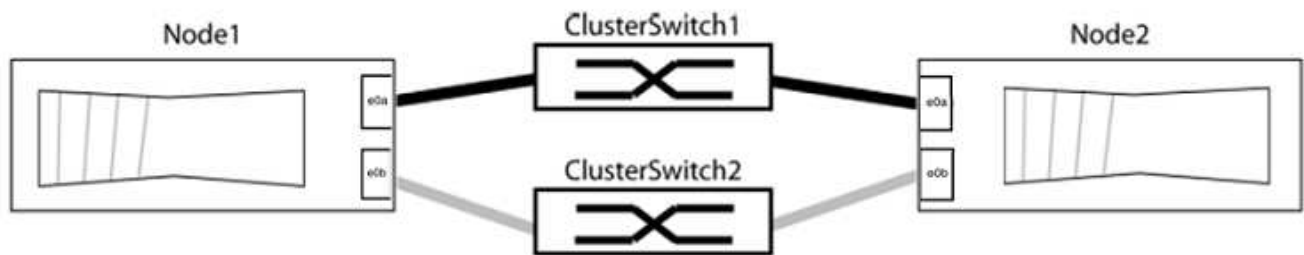
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Passaggio 2: configurare porte e cablaggio

1. Organizzare le porte del cluster su ogni switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano al cluster switch 1 e le porte del cluster nel gruppo 2 vadano al cluster switch 2. Questi gruppi saranno necessari più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e l'integrità del collegamento:

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

Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo è identificato come "nodo1:e0a" e "nodo2:e0a" e l'altro gruppo come "nodo1:e0b" e "nodo2:e0b". I nodi potrebbero utilizzare porte cluster diverse perché variano in base al sistema.



Verificare che le porte abbiano un valore di up per la colonna “Link” e un valore di healthy per la colonna “Stato di salute”.

Mostra esempio

```
cluster::> network port show -ipspace Cluster
```

```
Node: node1
```

```
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: node2
```

```
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
```

```
4 entries were displayed.
```

3. Verificare che tutti i LIF del cluster siano sulle rispettive porte home.

Verificare che la colonna "is-home" sia true per ciascuno dei LIF del cluster:

```
network interface show -vserver Cluster -fields is-home
```

Mostra esempio

```
cluster:*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif            is-home
-----  -
Cluster  node1_clus1    true
Cluster  node1_clus2    true
Cluster  node2_clus1    true
Cluster  node2_clus2    true
4 entries were displayed.
```

Se sono presenti LIF del cluster che non si trovano sulle loro porte home, ripristinare tali LIF sulle loro porte home:

```
network interface revert -vserver Cluster -lif *
```

4. Disabilitare il ripristino automatico per i LIF del cluster:

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

5. Verificare che tutte le porte elencate nel passaggio precedente siano connesse a uno switch di rete:

```
network device-discovery show -port cluster_port
```

La colonna "Dispositivo rilevato" dovrebbe contenere il nome dello switch del cluster a cui è connessa la porta.

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono collegate correttamente agli switch del cluster "cs1" e "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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 cluster sia integro:

```
cluster ring show
```

Tutte le unità devono essere master o secondarie.

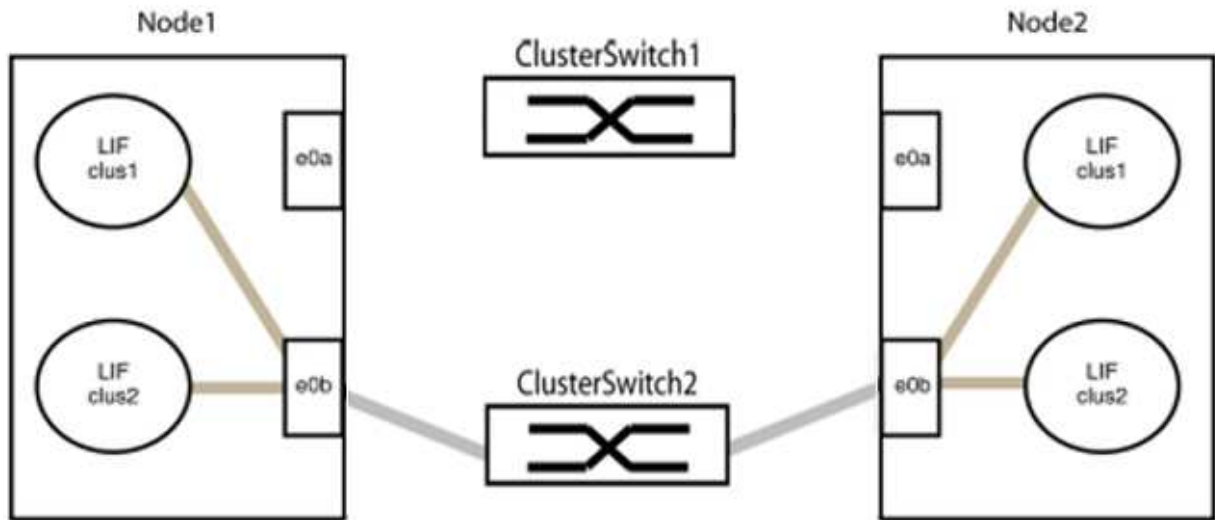
2. Impostare la configurazione senza switch per le porte del gruppo 1.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 1 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

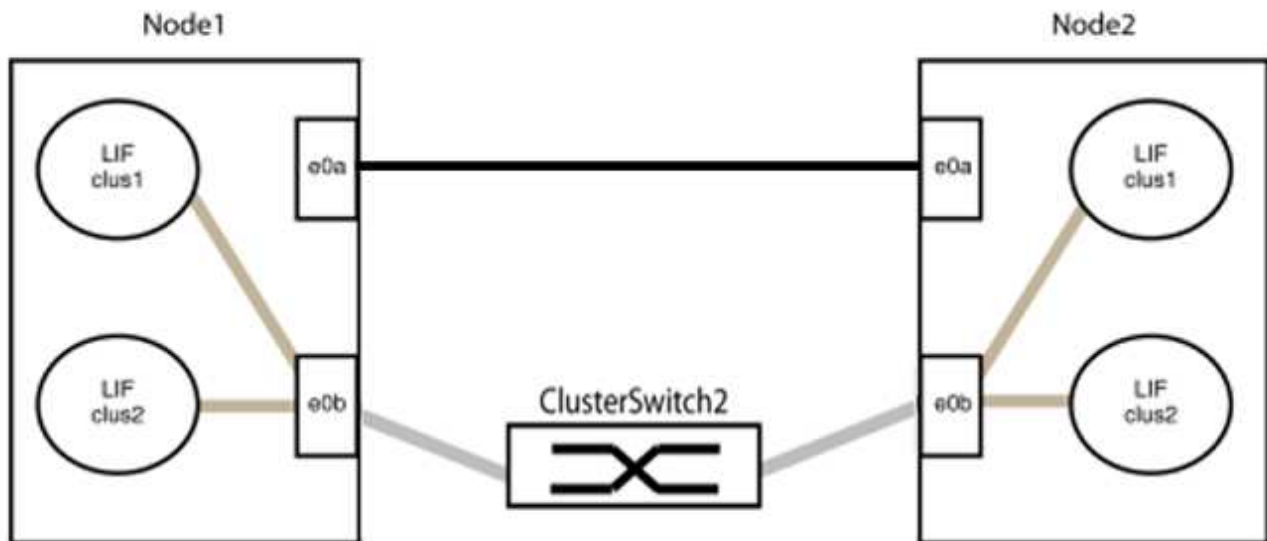
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 1.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0a" su ciascun nodo e il traffico del cluster continua attraverso lo switch e la porta "e0b" su ciascun nodo:



b. Collegare le porte del gruppo 1 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2:



3. L'opzione di rete cluster senza switch passa da `false` A `true` . L'operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione senza interruttore sia impostata su `true` :

```
network options switchless-cluster show
```

L'esempio seguente mostra che il cluster switchless è abilitato:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)

```



Prima di procedere al passaggio successivo, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

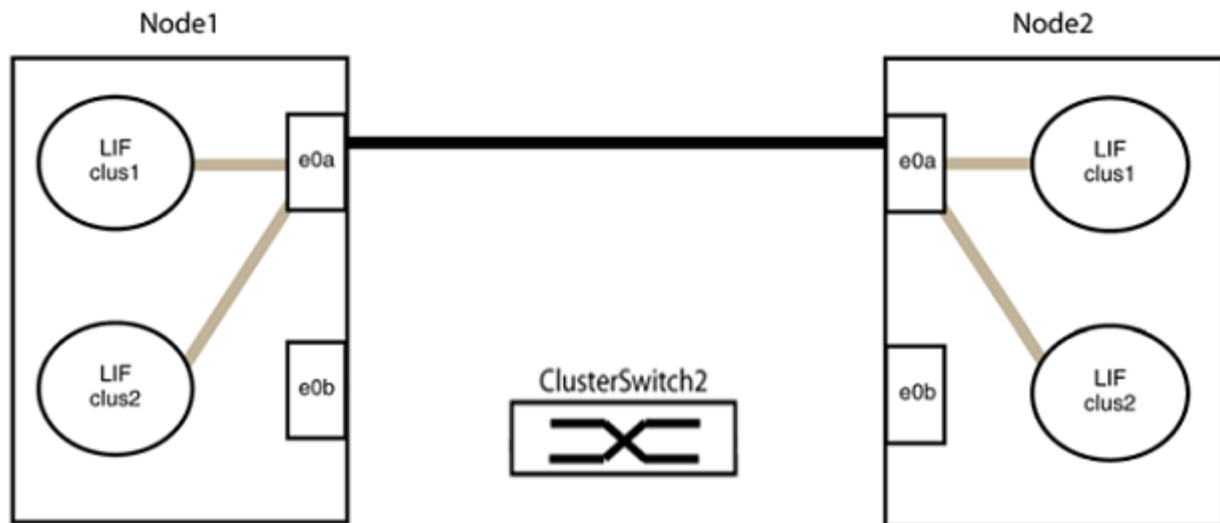
1. Impostare la configurazione senza switch per le porte nel gruppo 2.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

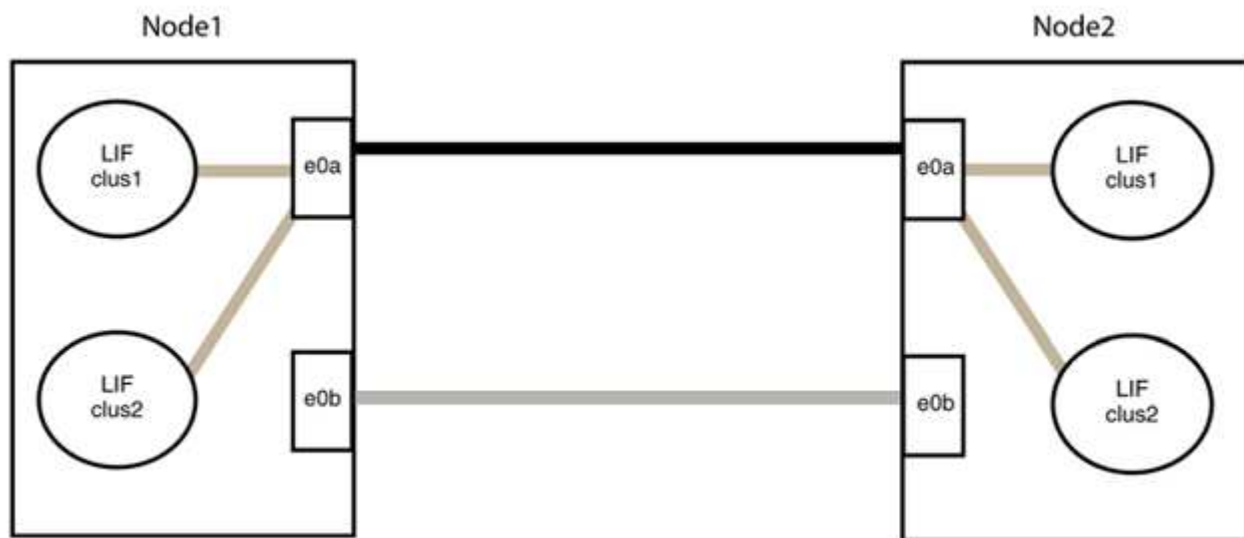
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 2.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua tramite la connessione diretta tra le porte "e0a":



b. Cablare le porte del gruppo 2 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2 e "e0b" sul nodo 1 è connesso a "e0b" sul nodo 2:



Passaggio 3: verificare la configurazione

1. Verificare che le porte su entrambi i nodi siano collegate correttamente:

```
network device-discovery show -port cluster_port
```

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono correttamente collegate alla porta corrispondente sul partner del cluster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e0a    node2                      e0a        AFF-A300
          e0b    node2                      e0b        AFF-A300
node1/lldp
          e0a    node2 (00:a0:98:da:16:44) e0a        -
          e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
          e0a    node1                      e0a        AFF-A300
          e0b    node1                      e0b        AFF-A300
node2/lldp
          e0a    node1 (00:a0:98:da:87:49) e0a        -
          e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Riattivare il ripristino automatico per i LIF del cluster:

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

3. Verificare che tutti i LIF siano a casa. Potrebbero volerci alcuni secondi.

```
network interface show -vserver Cluster -lif lif_name
```

Mostra esempio

I LIF sono stati ripristinati se la colonna "È a casa" è true , come mostrato per node1_clus2 E node2_clus2 nell'esempio seguente:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Se uno qualsiasi dei LIFS del cluster non è tornato alle proprie porte home, ripristinarlo manualmente dal nodo locale:

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

4. Controllare lo stato del cluster dei nodi dalla console di sistema di uno dei due nodi:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra epsilon su entrambi i nodi da false :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Per maggiori informazioni, vedere ["Articolo 1010449 della Knowledge Base NetApp : Come sopprimere la creazione automatica di casi durante le finestre di manutenzione programmata"](#).

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

NVIDIA SN2100

Iniziare

Flusso di lavoro di installazione e configurazione per gli switch NVIDIA SN2100

NVIDIA SN2100 è uno switch cluster che consente di creare cluster ONTAP con più di due nodi.

Segui questi passaggi del flusso di lavoro per installare e configurare gli switch NVIDIA SN2100.

1

"Rivedere i requisiti di configurazione"

Esaminare i requisiti di configurazione per lo switch cluster SN2100.

2

"Rivedere i componenti e i numeri delle parti"

Esaminare i componenti e i codici articolo dello switch cluster SN2100.

3

"Esaminare la documentazione richiesta"

Consultare la documentazione specifica dello switch e del controller per configurare gli switch SN2100 e il cluster ONTAP .

4

"Installare l'hardware"

Installare l'hardware dello switch.

5

"Configurare il software"

Configurare il software dello switch.

Requisiti di configurazione per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, assicurarsi di rivedere tutti i requisiti di configurazione.

Requisiti di installazione

Se si desidera creare cluster ONTAP con più di due nodi, sono necessari due switch di rete cluster supportati. È possibile utilizzare switch di gestione aggiuntivi, che sono facoltativi.

Installare lo switch NVIDIA SN2100 (X190006) nell'armadio switch doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Per le linee guida sul cablaggio, vedere ["Esaminare le considerazioni sul cablaggio e sulla configurazione"](#) .

Supporto ONTAP e Linux

Lo switch NVIDIA SN2100 è uno switch 10/25/40/100GbE che esegue Cumulus Linux. Lo switch supporta quanto segue:

- ONTAP 9.10.1P3 e versioni successive

Lo switch SN2100 supporta applicazioni Cluster e Storage in ONTAP 9.10.1P3 e versioni successive su diverse coppie di switch.

- Versioni del sistema operativo Cumulus Linux (CL)
 - Versioni CL specifiche sono qualificate e supportate da NetApp. Per informazioni sulla compatibilità attuale, vedere ["Informazioni sugli switch Ethernet NVIDIA"](#) pagina o la ["Hardware Universe NetApp"](#) .

- Per scaricare il software SN2100 Cumulus da NVIDIA, è necessario disporre delle credenziali di accesso per accedere al portale di supporto aziendale di NVIDIA. Vedi l'articolo della Knowledge Base ["Come registrarsi con NVIDIA per l'accesso al portale di supporto aziendale"](#).

- È possibile installare Cumulus Linux quando lo switch esegue Cumulus Linux o ONIE.

Cosa succederà ora?

Dopo aver esaminato i requisiti di configurazione, puoi confermare il tuo ["componenti e numeri di parte"](#).

Componenti e numeri di parte per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, assicurarsi di rivedere l'elenco dei componenti e i codici articolo del cabinet e del kit di guide.

Dettagli del mobile

Installare lo switch NVIDIA SN2100 (X190006) nell'armadio switch doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Dettagli del kit ferroviario

Nella tabella seguente sono elencati i codici articolo e la descrizione degli switch e dei kit di guide SN2100:

Numero di parte	Descrizione
X190006-PE	Switch cluster, NVIDIA SN2100, 16PT 100GbE, PTSX
X190006-PI	Switch cluster, NVIDIA SN2100, 16PT 100GbE, PSIN
X-MTEF-KIT-D	Kit di binari, NVIDIA Dual Switch affiancati
X-MTEF-KIT-E	Kit di guide, NVIDIA Single switch profondità ridotta



Per i dettagli, consultare la documentazione NVIDIA ["installazione del kit di switch e rail SN2100"](#).

Cosa succederà ora?

Dopo aver confermato i componenti e i numeri di parte, puoi rivedere il ["documentazione richiesta"](#).

Requisiti di documentazione per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, assicurarsi di consultare tutta la documentazione consigliata.

Titolo	Descrizione
"Guida all'installazione dello switch NVIDIA"	Descrive come installare gli switch NVIDIA SN2100.

Titolo	Descrizione
"Guida al cablaggio dello scaffale per unità NVMe NS224"	Panoramica e illustrazioni che mostrano come configurare il cablaggio per gli scaffali delle unità.
"Hardware Universe NetApp"	Consente di confermare l'hardware supportato, ad esempio switch e cavi di archiviazione, per il modello di piattaforma in uso.

Installare l'hardware

Flusso di lavoro di installazione hardware per switch NVIDIA SN2100

Per installare e configurare l'hardware per uno switch cluster SN2100, attenersi alla seguente procedura:

- 1** ["Installare l'hardware"](#)
 Installare l'hardware dello switch.
- 2** ["Esaminare le considerazioni sul cablaggio e sulla configurazione"](#)
 Esaminare i requisiti per le connessioni ottiche, l'adattatore QSA e la velocità dello switchport.
- 3** ["Cablare gli scaffali NS224"](#)
 Seguire le procedure di cablaggio se si dispone di un sistema in cui gli scaffali delle unità NS224 devono essere cablati come storage collegato allo switch (non come storage collegato direttamente).

Installare l'hardware per lo switch NVIDIA SN2100

Per installare l'hardware SN2100, fare riferimento alla documentazione NVIDIA.

Passi

1. Rivedere il ["requisiti di configurazione"](#).
2. Seguire le istruzioni in ["Guida all'installazione dello switch NVIDIA"](#).

Cosa succederà ora?

Dopo aver installato l'hardware, puoi ["rivedere il cablaggio e la configurazione"](#) requisiti.

Esaminare le considerazioni sul cablaggio e sulla configurazione

Prima di configurare lo switch NVIDIA SN2100, leggere le seguenti considerazioni.

Dettagli della porta NVIDIA

Porte di commutazione	Utilizzo delle porte
-----------------------	----------------------

swp1s0-3	4 nodi di porta del cluster breakout da 10 GbE
swp2s0-3	Nodi di porta del cluster breakout 4x25GbE
swp3-14	Nodi porta cluster 40/100GbE
swp15-16	Porte Inter-Switch Link (ISL) da 100 GbE

Vedi il ["Hardware Universe"](#) per maggiori informazioni sulle porte dello switch.

Ritardi di collegamento con connessioni ottiche

Se si verificano ritardi di collegamento superiori a cinque secondi, Cumulus Linux 5.4 e versioni successive includono il supporto per il collegamento rapido. È possibile configurare i collegamenti utilizzando `nv set` comando come segue:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Mostra esempio

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Supporto per connessioni in rame

Per risolvere questo problema sono necessarie le seguenti modifiche alla configurazione.

Cumulus Linux 4.4.3

1. Identificare il nome di ciascuna interfaccia utilizzando cavi in rame 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
```

Interface Vendor Rev	Identifier	Vendor Name	Vendor PN	Vendor SN
swp3 B0	0x11 (QSFP28)	Molex	112-00576	93A2229911111
swp4 B0	0x11 (QSFP28)	Molex	112-00576	93A2229922222

2. Aggiungere le due righe seguenti al `/etc/cumulus/switchd.conf` file per ogni porta (swp<n>) che utilizza cavi in rame 40GbE/100GbE:

```
° interface.swp<n>.enable_media_depended_linkup_flow=TRUE
```

```
° interface.swp<n>.enable_short_tuning=TRUE
```

Per esempio:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
```

```
.  
.  
interface.swp3.enable_media_depended_linkup_flow=TRUE  
interface.swp3.enable_short_tuning=TRUE  
interface.swp4.enable_media_depended_linkup_flow=TRUE  
interface.swp4.enable_short_tuning=TRUE
```

3. Riavviare il `switchd` servizio:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Verificare che le porte siano attive:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master: bridge(UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge(UP)

Cumulus Linux 5.x

1. Identificare il nome di ciascuna interfaccia utilizzando cavi in rame 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface --view=pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
swp3	0x11 (QSFP28)	Molex	112-00576	93A2229911111
B0				
swp4	0x11 (QSFP28)	Molex	112-00576	93A2229922222
B0				

2. Configurare i collegamenti utilizzando il `nv set` comando come segue:

- ° `nv set interface <interface-id> link fast-linkup on`
- ° `nv config apply`
- ° Ricarica il `switchd` servizio

Per esempio:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change
```

```
Are you sure? [y/N] y
applied [rev_id: 22]
```

```
Only switchd reload required
```

3. Verificare che le porte siano attive:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	-----
UP	swp3	100G	9216	Trunk/L2		Master: bridge(UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge(UP)

Vedi l'articolo della Knowledge Base ["Lo switch SN2100 non riesce a connettersi utilizzando cavi in rame 40/100GbE"](#) per ulteriori dettagli.

Su Cumulus Linux 4.4.2, le connessioni in rame non sono supportate sugli switch SN2100 con NIC X1151A, NIC X1146A o porte 100GbE integrate. Per esempio:

- AFF A800 sulle porte e0a ed e0b
- AFF A320 sulle porte e0g ed e0h

modulo QSA

Quando si utilizzano adattatori da QSFP+ (40GbE) a SFP+ (10GbE) o adattatori da QSFP28 (100GbE) a SFP28 (25GbE) (QSA), inserirli nelle porte dello switch 40GbE/100GbE non breakout (swp3-swp14). Non inserire il modulo QSA in una porta configurata per il breakout.

Quando si utilizza un modulo QSA per connettersi alle porte del cluster 10GbE/25GbE su una piattaforma, il collegamento potrebbe non essere attivo.

Per risolvere questo problema, procedere come segue:

- Per 10GbE, impostare manualmente la velocità di collegamento su 10000 e disattivare la negoziazione automatica.
- Per 25GbE, impostare manualmente la velocità di collegamento su 25000 e disattivare la negoziazione automatica.

Impostazione della velocità dell'interfaccia sulle porte breakout

A seconda del ricetrasmittitore nella porta dello switch, potrebbe essere necessario impostare la velocità sull'interfaccia dello switch su una velocità fissa. Se si utilizzano porte breakout da 10 GbE e 25 GbE o un modulo QSA, verificare che la negoziazione automatica sia disattivata e impostare la velocità dell'interfaccia sullo switch.

Cumulus Linux 4.4.3

Per esempio:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces      2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
    alias 10G Intra-Cluster Node
-   link-autoneg off
+   link-autoneg on
    link-speed 10000 <---- port speed set
    mstpctl-bpduguard yes
    mstpctl-portadminedge yes
    mtu 9216

auto swp2s0
iface swp2s0
    alias 25G Intra-Cluster Node
    link-autoneg off
    link-speed 25000 <---- port speed set
```

Controllare lo stato dell'interfaccia e della porta per verificare che le impostazioni siano state applicate:

```
cumulus@cumulus:mgmt:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	

.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

Cumulus Linux 5.x

Per esempio:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3
```

```
link
```

auto-negotiate	off	off
duplex	full	full
speed	10G	10G
fec	auto	auto
mtu	9216	9216
[breakout]		
state	up	up

Controllare lo stato dell'interfaccia e della porta per verificare che le impostazioni siano state applicate:

```
cumulus@cumulus:mgmt:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

Vedi il ["Hardware Universe"](#) e l'articolo della Knowledge Base ["Quali informazioni aggiuntive mi servono per installare la mia attrezzatura che non è in HWU?"](#) per maggiori informazioni.

Cosa succederà ora?

Dopo aver esaminato i requisiti di cablaggio e configurazione, è possibile ["cablare i ripiani NS224 come spazio di archiviazione collegato all'interruttore"](#).

Cablare gli scaffali NS224 come spazio di archiviazione collegato all'interruttore

Se si dispone di un sistema in cui gli scaffali delle unità NS224 devono essere cablati come storage collegato allo switch (non come storage collegato direttamente), utilizzare le informazioni fornite qui.

- Il cavo NS224 guida gli scaffali attraverso gli switch di archiviazione:

["Cablaggio degli scaffali dell'unità NS224 collegati all'interruttore"](#)

- Verifica l'hardware supportato, come switch e cavi di archiviazione, per il tuo modello di piattaforma:

["Hardware Universe NetApp"](#)

Cosa succederà ora?

Dopo aver cablato i tuoi scaffali, puoi ["configurare lo switch"](#).

Configurare il software

Flusso di lavoro di installazione del software per gli switch NVIDIA SN2100

Per installare e configurare il software per uno switch NVIDIA SN2100, seguire questi passaggi:

1

["Configurare l'interruttore"](#)

Configurare lo switch NVIDIA SN2100.

2

["Installa Cumulus Linux in modalità Cumulus"](#)

È possibile installare il sistema operativo Cumulus Linux (CL) quando lo switch esegue Cumulus Linux.

3

["Installa Cumulus Linux in modalità ONIE"](#)

In alternativa, è possibile installare il sistema operativo Cumulus Linux (CL) quando lo switch esegue Cumulus Linux in modalità ONIE.

4

["Aggiorna la tua versione di Cumulus Linux, se necessario"](#)

Puoi aggiornare il tuo sistema operativo Cumulus Linux (CL) in base alle tue esigenze.

5

["Installa o aggiorna lo script del file di configurazione di riferimento \(RCF\)"](#)

Sono disponibili due script RCF per le applicazioni di clustering e storage. La procedura è la stessa per entrambi.

6

["Installa il file CSHM"](#)

È possibile installare il file di configurazione applicabile per il monitoraggio dello stato degli switch Ethernet degli switch cluster NVIDIA .



"Ripristinare l'interruttore alle impostazioni predefinite di fabbrica"

Cancellare le impostazioni dello switch del cluster SN2100.

Configurare lo switch NVIDIA SN2100

Per configurare lo switch SN2100, fare riferimento alla documentazione NVIDIA.

Passi

1. Rivedere il ["requisiti di configurazione"](#) .
2. Seguire le istruzioni in ["Ripristino del sistema NVIDIA ."](#) .

Cosa succederà ora?

Dopo aver configurato lo switch, puoi ["installare Cumulus Linux in modalità Cumulus"](#) O ["installare Cumulus Linux in modalità ONIE"](#) .

Installa Cumulus Linux in modalità Cumulus

Seguire questa procedura per installare il sistema operativo Cumulus Linux (CL) quando lo switch è in esecuzione in modalità Cumulus.



Il sistema operativo Cumulus Linux (CL) può essere installato quando lo switch esegue Cumulus Linux o ONIE (vedere ["Installa in modalità ONIE"](#)).

Prima di iniziare

Assicurati di avere quanto segue:

- Conoscenza di Linux di livello intermedio.
- Familiarità con le nozioni di base di modifica del testo, autorizzazioni dei file UNIX e monitoraggio dei processi. Sono preinstallati diversi editor di testo, tra cui `vi` E `nano` .
- Accesso a una shell Linux o UNIX. Se utilizzi Windows, utilizza un ambiente Linux come strumento da riga di comando per interagire con Cumulus Linux.
- Il requisito di velocità in baud è impostato su 115200 sullo switch della console seriale per l'accesso alla console dello switch NVIDIA SN2100, come segue:
 - 115200 baud
 - 8 bit di dati
 - 1 bit di stop
 - parità: nessuna
 - controllo di flusso: nessuno

Informazioni su questo compito

Siate consapevoli di quanto segue:



Ogni volta che Cumulus Linux viene installato, l'intera struttura del file system viene cancellata e ricostruita.



La password predefinita per l'account utente Cumulus è **cumulus**. La prima volta che accedi a Cumulus Linux, devi modificare questa password predefinita. Assicurati di aggiornare tutti gli script di automazione prima di installare una nuova immagine. Cumulus Linux fornisce opzioni da riga di comando per modificare automaticamente la password predefinita durante il processo di installazione.

Esempio 1. Passi

Cumulus Linux 4.4.3

1. Accedi allo switch.

Il primo accesso allo switch richiede nome utente/password **cumulus/cumulus** con sudo privilegi.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Controlla la versione di Cumulus Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configurare il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito. Il nuovo nome host diventa effettivo solo dopo aver riavviato la console/sessione SSH.



Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificatamente destinata alla gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.



Non utilizzare caratteri di sottolineatura (_), apostrofo (') o caratteri non ASCII nel nome host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Questo comando modifica entrambi i `/etc/hostname` e `/etc/hosts` file.

4. Verificare che il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito siano stati aggiornati.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Impostare la data, l'ora, il fuso orario e il server NTP sullo switch.

- a. Verifica il fuso orario attuale:

```
cumulus@sw1:~$ cat /etc/timezone
```

- b. Aggiornamento al nuovo fuso orario:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Verifica il tuo fuso orario attuale:

```
cumulus@switch:~$ date +%Z
```

d. Per impostare il fuso orario tramite la procedura guidata, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Imposta l'orologio del software in base al fuso orario configurato:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Imposta il valore corrente dell'orologio software sull'orologio hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Aggiungere un server NTP se necessario:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>  
iburst  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

h. Verificare che ntpd è in esecuzione sul sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp  
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p  
/var/run/ntpd.pid -g -u 101:102
```

i. Specificare l'interfaccia sorgente NTP. Per impostazione predefinita, l'interfaccia sorgente utilizzata da NTP è eth0. È possibile configurare un'interfaccia sorgente NTP diversa come segue:

```
cumulus@sw1:~$ net add time ntp source <src_int>  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

6. Installa Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

Il programma di installazione avvia il download. Quando richiesto, digitare **y**.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione si avvia automaticamente e vengono visualizzate le seguenti opzioni della schermata GRUB. **Non** effettuare alcuna selezione.

- Cumulus-Linux GNU/Linux
- ONIE: Installa il sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Ripetere i passaggi da 1 a 4 per effettuare l'accesso.

10. Verificare che la versione di Cumulus Linux sia 4.4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Crea un nuovo utente e aggiungilo a `sudo` gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

Cumulus Linux 5.4.0

1. Accedi allo switch.

Il primo accesso allo switch richiede nome utente/password **cumulus/cumulus** con sudo privilegi.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Controlla la versione di Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.3.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configurare il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito. Il nuovo nome host diventa effettivo solo dopo aver riavviato la console/sessione SSH.



Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificatamente destinata alla gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.



Non utilizzare caratteri di sottolineatura (`_`), apostrofo (`'`) o caratteri non ASCII nel nome host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Questo comando modifica entrambi i `/etc/hostname` e `/etc/hosts` file.

4. Verificare che il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito siano stati aggiornati.

```

cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1

```

5. Impostare il fuso orario, la data, l'ora e il server NTP sullo switch.

a. Imposta il fuso orario:

```

cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply

```

b. Verifica il tuo fuso orario attuale:

```

cumulus@switch:~$ date +%Z

```

c. Per impostare il fuso orario tramite la procedura guidata, eseguire il seguente comando:

```

cumulus@sw1:~$ sudo dpkg-reconfigure tzdata

```

d. Imposta l'orologio del software in base al fuso orario configurato:

```

cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"

```

e. Imposta il valore corrente dell'orologio software sull'orologio hardware:

```

cumulus@sw1:~$ sudo hwclock -w

```

f. Aggiungere un server NTP se necessario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Vedi l'articolo della Knowledge Base ["La configurazione del server NTP non funziona con gli switch NVIDIA SN2100"](#) per ulteriori dettagli.

g. Verificare che ntpd è in esecuzione sul sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Specificare l'interfaccia sorgente NTP. Per impostazione predefinita, l'interfaccia sorgente utilizzata da NTP è `eth0`. È possibile configurare un'interfaccia sorgente NTP diversa come segue:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installa Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

Il programma di installazione avvia il download. Quando richiesto, digitare **y**.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione si avvia automaticamente e vengono visualizzate le seguenti opzioni della schermata GRUB. **Non** effettuare alcuna selezione.

- Cumulus-Linux GNU/Linux
- ONIE: Installa il sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Ripetere i passaggi da 1 a 4 per effettuare l'accesso.

10. Verificare che la versione di Cumulus Linux sia 5.4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 13:37:36	system uptime
timezone	Etc/UTC	system time zone

11. Verificare che ciascun nodo abbia una connessione con ciascun switch:

```
cumulus@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			
eth0	100M	Mgmt	mgmt-sw1
Eth110/1/29			
swp2s1	25G	Trunk/L2	node1
e0a			
swp15	100G	BondMember	sw2
swp15			
swp16	100G	BondMember	sw2
swp16			

12. Crea un nuovo utente e aggiungilo a sudo gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

13. Aggiungere gruppi di utenti aggiuntivi a cui l'utente amministratore può accedere `nv` comandi:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user 'admin' to group 'nvshow' ...
Adding user admin to group nvshow
Done.
```

Vedere ["Account utente NVIDIA"](#) per maggiori informazioni.

Cumulus Linux 5.11.0

1. Accedi allo switch.

Quando si accede allo switch per la prima volta, è necessario il nome utente/password di **cumulus** /**cumulus** con sudo privilegi.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Controlla la versione di Cumulus Linux: nv show system

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configurare il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito. Il nuovo nome host diventa effettivo solo dopo aver riavviato la console/sessione SSH.



Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificatamente destinata alla gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.



Non utilizzare caratteri di sottolineatura (`_`), apostrofo (`'`) o caratteri non ASCII nel nome host.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Questo comando modifica entrambi i /etc/hostname E /etc/hosts file.

4. Verificare che il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito siano stati aggiornati.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Impostare il fuso orario, la data, l'ora e il server NTP sullo switch.

- a. Imposta il fuso orario:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

- b. Verifica il tuo fuso orario attuale:

```
cumulus@switch:~$ date +%Z
```

- c. Per impostare il fuso orario tramite la procedura guidata, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- d. Imposta l'orologio del software in base al fuso orario configurato:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

- e. Imposta il valore corrente dell'orologio software sull'orologio hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

- f. Aggiungere un server NTP se necessario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Vedi l'articolo della Knowledge Base ["La configurazione del server NTP non funziona con gli switch NVIDIA SN2100"](#) per ulteriori dettagli.

- g. Verificare che ntpd è in esecuzione sul sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

- h. Specificare l'interfaccia sorgente NTP. Per impostazione predefinita, l'interfaccia sorgente utilizzata da NTP è `eth0`. È possibile configurare un'interfaccia sorgente NTP diversa come segue:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installa Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

Il programma di installazione avvia il download. Quando richiesto, digitare `y`.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione si avvia automaticamente e vengono visualizzate le seguenti opzioni della schermata GRUB. **Non** effettuare alcuna selezione.

- Cumulus-Linux GNU/Linux
- ONIE: Installa il sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Ripetere i passaggi da 1 a 4 per effettuare l'accesso.

10. Verificare che la versione di Cumulus Linux sia 5.11.0:

```
nv show system
```

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
-----	-----	-----
build	Cumulus Linux 5.11.0	
uptime	153 days, 2:44:16	
hostname	cumulus	cumulus
product-name	Cumulus Linux	
product-release	5.11.0	
platform	x86_64-mlnx_x86-r0	
system-memory	2.76 GB used / 2.28 GB free / 7.47 GB total	
swap-memory	0 Bytes used / 0 Bytes free / 0 Bytes total	
health-status	not OK	
date-time	2025-04-23 09:55:24	
status	N/A	
timezone	Etc/UTC	
maintenance		
mode	disabled	
ports	enabled	
version		
kernel	6.1.0-cl-1-amd64	
build-date	Thu Nov 14 13:06:38 UTC 2024	
image	5.11.0	
onie	2019.11-5.2.0020-115200	

11. Verificare che ogni nodo abbia una connessione a ogni switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			

eth0	100M	eth	mgmt-sw1
Eth110/1/14			
swp2s1	25G	Trunk/L2	node1
e0a			
swp1s1	10G	swp	sw2
e0a			
swp9	100G	swp	sw3
e4a			
swp10	100G	swp	sw4
e4a			
swp15	100G	swp	sw5
swp15			
swp16	100G	swp	sw6
swp16			

Vedere ["Account utente NVIDIA"](#) per maggiori informazioni.

Cosa succederà ora?

Dopo aver installato Cumulus Linux in modalità Cumulus, ["installare lo script del file di configurazione di riferimento \(RCF\)"](#).

Installa Cumulus Linux in modalità ONIE

Seguire questa procedura per installare il sistema operativo Cumulus Linux (CL) quando lo switch è in esecuzione in modalità ONIE.



Il sistema operativo Cumulus Linux (CL) può essere installato quando lo switch esegue ONIE o Cumulus Linux (vedere ["Installa in modalità Cumulus"](#)).

Informazioni su questo compito

È possibile installare Cumulus Linux utilizzando Open Network Install Environment (ONIE), che consente il rilevamento automatico di un'immagine di installazione di rete. Ciò semplifica il modello di sistema di protezione degli switch con la scelta di un sistema operativo, come Cumulus Linux. Il modo più semplice per installare Cumulus Linux con ONIE è tramite la scoperta HTTP locale.



Se il tuo host è abilitato per IPv6, assicurati che esegua un server web. Se il tuo host è abilitato per IPv4, assicurati che esegua DHCP oltre a un server web.

Questa procedura illustra come aggiornare Cumulus Linux dopo che l'amministratore ha avviato ONIE.

Esempio 2. Passi

Cumulus Linux 4.4.3

1. Scaricare il file di installazione di Cumulus Linux nella directory principale del server web. Rinomina questo file in: `onie-installer`.
2. Collegare l'host alla porta Ethernet di gestione dello switch tramite un cavo Ethernet.
3. Accendere l'interruttore.

Lo switch scarica il programma di installazione dell'immagine ONIE e si avvia. Una volta completata l'installazione, nella finestra del terminale verrà visualizzato il prompt di accesso a Cumulus Linux.



Ogni volta che Cumulus Linux viene installato, l'intera struttura del file system viene cancellata e ricostruita.

4. Riavviare lo switch SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Premere il tasto **Esc** nella schermata GNU GRUB per interrompere il normale processo di avvio, selezionare **ONIE** e premere **Invio**.
6. Nella schermata successiva, seleziona **ONIE: Installa SO**.
7. Il processo di rilevamento del programma di installazione ONIE viene eseguito alla ricerca dell'installazione automatica. Premere **Invio** per interrompere temporaneamente il processo.
8. Quando il processo di scoperta si è interrotto:

```
ONIE:/ # onie-stop  
discover: installer mode detected.  
Stopping: discover...start-stop-daemon: warning: killing process  
427:  
No such process done.
```

9. Se il servizio DHCP è in esecuzione sulla rete, verificare che l'indirizzo IP, la subnet mask e il gateway predefinito siano assegnati correttamente:

```
ifconfig eth0
```

```

ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
        TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
        Memory:dfc00000-dfc1ffff

```

```

ONIE:/ # route
Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	Metric	Ref
Use Iface					
default	10.233.204.1	0.0.0.0	UG	0	0
0 eth0					
10.233.204.0	*	255.255.254.0	U	0	0
0 eth0					

10. Se lo schema di indirizzamento IP è definito manualmente, procedere come segue:

```

ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1

```

11. Ripetere il passaggio 9 per verificare che le informazioni statiche siano state immesse correttamente.

12. Installa Cumulus Linux:

```

# onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-
mlx-amd64.bin

```

```

ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-4.4.3-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-
4.4.3-mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*|    552M  0:00:00 ETA
...
...

```

13. Una volta completata l'installazione, accedi allo switch.

```

cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>

```

14. Verificare la versione di Cumulus Linux: `net show version`

```

cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"

```

Cumulus Linux 5.x

1. Scaricare il file di installazione di Cumulus Linux nella directory principale del server web. Rinomina questo file in: `onie-installer`.
2. Collegare l'host alla porta Ethernet di gestione dello switch tramite un cavo Ethernet.
3. Accendere l'interruttore.

Lo switch scarica il programma di installazione dell'immagine ONIE e si avvia. Una volta completata l'installazione, nella finestra del terminale verrà visualizzato il prompt di accesso a Cumulus Linux.



Ogni volta che Cumulus Linux viene installato, l'intera struttura del file system viene cancellata e ricostruita.

4. Riavviare lo switch SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
.
.
GNU GRUB version 2.06-3
+-----+
-----+
| Cumulus-Linux GNU/Linux
|
| Advanced options for Cumulus-Linux GNU/Linux
|
| ONIE
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
+-----+
-----+
```

5. Premere il tasto Esc nella schermata GNU GRUB per interrompere il normale processo di avvio, selezionare ONIE e premere Invio.

```

.
.
Loading ONIE ...

GNU GRUB version 2.02
+-----+
-----+
| ONIE: Install OS
|
| ONIE: Rescue
|
| ONIE: Uninstall OS
|
| ONIE: Update ONIE
|
| ONIE: Embed ONIE
|
|
|
|
|
|
|
|
|
|
|
+-----+
-----+

```

Seleziona ONIE: **Installa sistema operativo.**

6. Il processo di rilevamento del programma di installazione ONIE viene eseguito alla ricerca dell'installazione automatica. Premere **Invio** per interrompere temporaneamente il processo.
7. Quando il processo di scoperta si è interrotto:

```

ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process
427:
No such process done.

```

8. Configurare l'indirizzo IP, la subnet mask e il gateway predefinito:

```
ifconfig eth0
```

```

ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
        TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
        Memory:dfc00000-dfc1ffff

ONIE:/ #
ONIE:/ # ifconfig eth0 10.228.140.27 netmask 255.255.248.0
ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet HWaddr B8:CE:F6:5E:05:E6
        inet addr:10.228.140.27 Bcast:10.228.143.255
Mask:255.255.248.0
        inet6 addr: fd20:8b1e:b255:822b:bace:f6ff:fe5e:5e6/64
Scope:Global
        inet6 addr: fe80::bace:f6ff:fe5e:5e6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:18813 errors:0 dropped:1418 overruns:0 frame:0
        TX packets:491 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1339596 (1.2 MiB) TX bytes:49379 (48.2 KiB)
        Memory:dfc00000-dfc1ffff

ONIE:/ # route add default gw 10.228.136.1
ONIE:/ # route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref
Use Iface

default          10.228.136.1    0.0.0.0          UG      0      0
0 eth0
10.228.136.1     *               255.255.248.0    U        0      0
0 eth0

```

9. Installa Cumulus Linux 5.4:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

```

ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-5.4-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-5.4-
mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*|    552M  0:00:00 ETA
...
...

```

10. Una volta completata l'installazione, accedi allo switch.

```

cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>

```

11. Verificare la versione di Cumulus Linux: `nv show system`

```

cumulus@cumulus:mgmt:~$ nv show system
operational      applied          description
-----
hostname         cumulus         cumulus
build            Cumulus Linux 5.4.0  system build version
uptime          6 days, 13:37:36  system uptime
timezone        Etc/UTC         system time zone

```

12. Crea un nuovo utente e aggiungilo a sudo gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```

sudo adduser --ingroup netedit admin

```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

13. Aggiungere gruppi di utenti aggiuntivi a cui l'utente amministratore può accedere `nv` comandi:

```
cumulus@cumulus:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Vedere ["Account utente NVIDIA"](#) per maggiori informazioni.

Cosa succederà ora?

Dopo aver installato Cumulus Linux in modalità ONIE, puoi ["installare lo script del file di configurazione di riferimento \(RCF\)"](#).

Aggiorna le versioni di Cumulus Linux

Completa la seguente procedura per aggiornare la tua versione di Cumulus Linux come richiesto.

Prima di iniziare

Assicurati di avere quanto segue:

- Conoscenza di Linux di livello intermedio.
- Familiarità con le nozioni di base di modifica del testo, autorizzazioni dei file UNIX e monitoraggio dei processi. Sono preinstallati diversi editor di testo, tra cui `vi` e `nano`.
- Accesso a una shell Linux o UNIX. Se utilizzi Windows, utilizza un ambiente Linux come strumento da riga di comando per interagire con Cumulus Linux.
- Il requisito di velocità in baud è impostato su 115200 sullo switch della console seriale per l'accesso alla console dello switch NVIDIA SN2100, come segue:
 - 115200 baud
 - 8 bit di dati
 - 1 bit di stop
 - parità: nessuna
 - controllo di flusso: nessuno

Informazioni su questo compito

Siate consapevoli di quanto segue:



Ogni volta che Cumulus Linux viene aggiornato, l'intera struttura del file system viene cancellata e ricostruita. La configurazione esistente verrà cancellata. Prima di aggiornare Cumulus Linux, è necessario salvare e registrare la configurazione dello switch.



La password predefinita per l'account utente Cumulus è **cumulus**. La prima volta che accedi a Cumulus Linux, devi modificare questa password predefinita. È necessario aggiornare tutti gli script di automazione prima di installare una nuova immagine. Cumulus Linux fornisce opzioni da riga di comando per modificare automaticamente la password predefinita durante il processo di installazione.

Vedere "[Installazione di una nuova immagine Cumulus Linux](#)" per ulteriori informazioni.

Esempio 3. Passi

Da Cumulus Linux 4.4.x a Cumulus Linux 5.4.0

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il comando ping per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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. Controlla la versione corrente di Cumulus Linux e le porte connesse:

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

```
cumulus@cumulus:mgmt:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

.					
.					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
.					
.					

7. Scarica l'immagine Cumulux Linux 5.4.0:

```
cumulus@cumulus:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Riavviare lo switch:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

9. Cambia la password:

```

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

```

10. Controlla la versione di Cumulus Linux: `nv show system`

```

cumulus@cumulus:mgmt:~$ nv show system

```

	operational	applied
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	
uptime	14:07:08	
timezone	Etc/UTC	

11. Cambia il nome host:

```

cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.

```

12. Disconnettersi e accedere nuovamente allo switch per visualizzare il nome dello switch aggiornato al prompt:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Imposta l'indirizzo IP:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Crea un nuovo utente e aggiungilo a sudo gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

15. Aggiungere gruppi di utenti aggiuntivi a cui l'utente amministratore può accedere `nv` comandi:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Vedere ["Account utente NVIDIA"](#) per maggiori informazioni.

Da Cumulus Linux 5.x a Cumulus Linux 5.4.0

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il comando ping per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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. Controlla la versione corrente di Cumulus Linux e le porte connesse:

```

cumulus@sw1:mgmt:~$ nv show system
                                operational          applied
-----
hostname                        cumulus              cumulus
build                          Cumulus Linux 5.3.0
uptime                          6 days, 8:37:36
timezone                        Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216  200G  up
bond
+ eth0          1500  100M  up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536      up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216  10G   up    cluster01         e0b
swp
.
.
.
+ swp15         9216  100G   up    sw2                swp15
swp
+ swp16         9216  100G   up    sw2                swp16
swp

```

7. Scarica l'immagine Cumulux Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Riavviare lo switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Cambia la password:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Controlla la versione di Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied
-----
hostname         cumulus cumulus
build            Cumulus Linux 5.4.0
uptime           14:07:08
timezone         Etc/UTC
```

11. Cambia il nome host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.
```

12. Disconnettersi e riconnettersi allo switch per visualizzare il nome dello switch aggiornato nel prompt:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Imposta l'indirizzo IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Crea un nuovo utente e aggiungilo a sudo gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

15. Aggiungere gruppi di utenti aggiuntivi a cui l'utente amministratore può accedere `nv` comandi:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Vedere ["Account utente NVIDIA"](#) per maggiori informazioni.

Da Cumulus Linux 5.4.0 a Cumulus Linux 5.11.0

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il comando ping per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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. Controlla la versione corrente di Cumulus Linux e le porte connesse:

```

cumulus@sw1:mgmt:~$ nv show system
                                operational          applied
-----
hostname                        cumulus              cumulus
build                          Cumulus Linux 5.4.0
uptime                          6 days, 8:37:36
timezone                        Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216   200G   up
bond
+ eth0          1500   100M   up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536   up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216   10G    up    cluster01         e0b
swp
.
.
.
+ swp15         9216   100G   up    sw2                swp15
swp
+ swp16         9216   100G   up    sw2                swp16
swp

```

7. Scarica l'immagine Cumulux Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Riavviare lo switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Cambia la password:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Controlla la versione di Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied
-----
hostname         cumulus cumulus
build            Cumulus Linux 5.11.0
uptime           14:07:08
timezone         Etc/UTC
```

11. Cambia il nome host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.
```

12. Disconnettersi e riconnettersi allo switch per visualizzare il nome dello switch aggiornato nel prompt:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Imposta l'indirizzo IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

Cosa succederà ora?

Dopo aver aggiornato la versione di Cumulus Linux, puoi [installare o aggiornare lo script RCF](#) .

Installa o aggiorna lo script del file di configurazione di riferimento (RCF)

Seguire questa procedura per installare o aggiornare lo script RCF.

Prima di iniziare

Prima di installare o aggiornare lo script RCF, assicurarsi che sullo switch siano disponibili i seguenti elementi:

- Cumulus Linux è installato. Vedi il ["Hardware Universe"](#) per le versioni supportate.
- Indirizzo IP, maschera di sottorete e gateway predefinito definiti tramite DHCP o configurati manualmente.



È necessario specificare un utente nel RCF (oltre all'utente amministratore) da utilizzare specificamente per la raccolta dei log.

Configurazioni del cliente

Sono disponibili le seguenti categorie di configurazione di riferimento:

Grappolo	Sulle porte configurate per il breakout 4x10GbE, una porta è configurata per il breakout 4x25GbE e le altre porte sono configurate per 40/100GbE. Supporta il traffico cluster/HA condiviso sulle porte per i nodi che utilizzano porte cluster/HA condivise. Consultare la tabella delle piattaforme nell'articolo della Knowledge Base " Quali piattaforme AFF, ASA e FAS utilizzano porte Ethernet Cluster e HA condivise? ". Tutte le porte possono essere utilizzate anche come porte cluster dedicate.
Magazzinaggio	Tutte le porte sono configurate per connessioni di archiviazione NVMe da 100 GbE.

Versioni attuali dello script RCF

Sono disponibili due script RCF per le applicazioni Cluster e Storage. Scarica RCF da "[Download del software NVIDIA SN2100](#)" pagina. La procedura è la stessa per entrambi.

- Cluster: **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**
- Archiviazione: **MSN2100-RCF-v1.x-Archiviazione**

Informazioni sugli esempi

La seguente procedura di esempio mostra come scaricare e applicare lo script RCF per gli switch Cluster.

L'output del comando di esempio utilizza l'indirizzo IP di gestione dello switch 10.233.204.71, la netmask 255.255.254.0 e il gateway predefinito 10.233.204.1.

Esempio 4. Passi

Cumulus Linux 4.4.3

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il `ping` comando per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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
```

- Se stai aggiornando il tuo RCF, devi disabilitare il ripristino automatico per questo passaggio.
- Se hai appena aggiornato la tua versione di Cumulus Linux, non è necessario disattivare il ripristino automatico per questo passaggio perché è già disattivato.

1. Visualizza le interfacce disponibili sullo switch SN2100:

```
admin@sw1:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	---	-----	-----	-----	-----
-----	-----	---	-----	-----	-----	-----
...						
...						
ADMDN	swp1	N/A	9216	NotConfigured		
ADMDN	swp2	N/A	9216	NotConfigured		
ADMDN	swp3	N/A	9216	NotConfigured		
ADMDN	swp4	N/A	9216	NotConfigured		
ADMDN	swp5	N/A	9216	NotConfigured		
ADMDN	swp6	N/A	9216	NotConfigured		
ADMDN	swp7	N/A	9216	NotConfigured		
ADMDN	swp8	N/A	9216	NotConfigured		
ADMDN	swp9	N/A	9216	NotConfigured		
ADMDN	swp10	N/A	9216	NotConfigured		
ADMDN	swp11	N/A	9216	NotConfigured		
ADMDN	swp12	N/A	9216	NotConfigured		
ADMDN	swp13	N/A	9216	NotConfigured		
ADMDN	swp14	N/A	9216	NotConfigured		
ADMDN	swp15	N/A	9216	NotConfigured		
ADMDN	swp16	N/A	9216	NotConfigured		

2. Copiare lo script RCF Python sullo switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



Mentre `scp` viene utilizzato nell'esempio, puoi usare il tuo metodo preferito per il trasferimento dei file, ad esempio SFTP, HTTPS o FTP.

3. Applicare lo script python RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Lo script RCF completa i passaggi elencati nell'esempio precedente.



Nel passaggio 3 **Aggiornamento del file MOTD** sopra, il comando `cat /etc/motd` è in esecuzione. Ciò consente di verificare il nome del file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.



Per qualsiasi problema relativo allo script python RCF che non può essere corretto, contattare ["Supporto NetApp"](#) per assistenza.

4. 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.
5. Verificare la configurazione dopo il riavvio:

```
admin@sw1:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
...						
...						
DN	swp1s0	N/A	9216	Trunk/L2		Master:
	bridge (UP)					
DN	swp1s1	N/A	9216	Trunk/L2		Master:
	bridge (UP)					
DN	swp1s2	N/A	9216	Trunk/L2		Master:
	bridge (UP)					
DN	swp1s3	N/A	9216	Trunk/L2		Master:

```

bridge (UP)
DN      swp2s0      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s1      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s2      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s3      N/A      9216      Trunk/L2      Master:
bridge (UP)
UP      swp3         100G     9216      Trunk/L2      Master:
bridge (UP)
UP      swp4         100G     9216      Trunk/L2      Master:
bridge (UP)
DN      swp5         N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp6         N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp7         N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp8         N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp9         N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp10        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp11        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp12        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp13        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp14        N/A      9216      Trunk/L2      Master:
bridge (UP)
UP      swp15        N/A      9216      BondMember    Master:
bond_15_16 (UP)
UP      swp16        N/A      9216      BondMember    Master:
bond_15_16 (UP)
...
...

```

```
admin@sw1:mgmt:~$ net show roce config
```

```
RoCE mode..... lossless
```

```
Congestion Control:
```

```
Enabled SPs.... 0 2 5
```

```
Mode..... ECN
```

```
Min Threshold.. 150 KB
```

```

Max Threshold.. 1500 KB
PFC:
  Status..... enabled
  Enabled SPs.... 2 5
  Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9

```

DSCP	802.1p	switch-priority
-----	-----	-----
0 1 2 3 4 5 6 7	0	0
8 9 10 11 12 13 14 15	1	1
16 17 18 19 20 21 22 23	2	2
24 25 26 27 28 29 30 31	3	3
32 33 34 35 36 37 38 39	4	4
40 41 42 43 44 45 46 47	5	5
48 49 50 51 52 53 54 55	6	6
56 57 58 59 60 61 62 63	7	7

switch-priority	TC	ETS
-----	--	-----
0 1 3 4 6 7	0	DWRR 28%
2	2	DWRR 28%
5	5	DWRR 43%

6. Verificare le informazioni per il ricetrasmittitore nell'interfaccia:

```

admin@sw1:mgmt:~$ net show interface pluggables
Interface  Identifier      Vendor Name  Vendor PN      Vendor SN
Vendor Rev
-----
swp3       0x11 (QSFP28)  Amphenol    112-00574
APF20379253516 B0
swp4       0x11 (QSFP28)  AVAGO       332-00440      AF1815GU05Z
A0
swp15      0x11 (QSFP28)  Amphenol    112-00573
APF21109348001 B0
swp16      0x11 (QSFP28)  Amphenol    112-00573
APF21109347895 B0

```

7. Verificare che ciascun nodo abbia una connessione con ciascun switch:

```
admin@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	sw1	e3a
swp4	100G	Trunk/L2	sw2	e3b
swp15	100G	BondMember	sw13	swp15
swp16	100G	BondMember	sw14	swp16

8. 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:

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

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

b. Verificare lo stato di integrità dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono posizionati su e0d).

```

cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface Platform
-----
node1/lldp
          e3a    sw1  (b8:ce:f6:19:1a:7e)    swp3      -
          e3b    sw2  (b8:ce:f6:19:1b:96)    swp3      -

node2/lldp
          e3a    sw1  (b8:ce:f6:19:1a:7e)    swp4      -
          e3b    sw2  (b8:ce:f6:19:1b:96)    swp4      -

cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                                     Type                               Address
Model
-----
-----
sw1                                         cluster-network                    10.233.205.90
MSN2100-CB2RC
    Serial Number: MNXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                                         cluster-network                    10.233.205.91
MSN2100-CB2RC
    Serial Number: MNCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

```

9. Verificare che il cluster sia integro:

```
cluster show
```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.

11. Abilita il ripristino automatico sui LIF del cluster.

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

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il ping comando per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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
```

- Se stai aggiornando il tuo RCF, devi disabilitare il ripristino automatico per questo passaggio.
- Se hai appena aggiornato la tua versione di Cumulus Linux, non è necessario disattivare il ripristino automatico per questo passaggio perché è già disattivato.

1. Visualizza le interfacce disponibili sullo switch SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216   200G   up
bond
+ eth0          1500   100M   up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216   10G    up    cluster01         e0b
swp
.
.
.
+ swp15         9216   100G    up    sw2                swp15
swp
+ swp16         9216   100G    up    sw2                swp16
swp
```

2. Copiare lo script RCF Python sullo switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



Mentre `scp` viene utilizzato nell'esempio, puoi usare il tuo metodo preferito per il trasferimento dei file, ad esempio SFTP, HTTPS o FTP.

3. Applicare lo script python RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Lo script RCF completa i passaggi elencati nell'esempio precedente.



Nel passaggio 3 **Aggiornamento del file MOTD** sopra, il comando `cat /etc/issue.net` è in esecuzione. Ciò consente di verificare il nome del file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.

Per esempio:

```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1       : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2       : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



Per qualsiasi problema relativo allo script python RCF che non può essere corretto, contattare ["Supporto NetApp"](#) per assistenza.

4. 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.
5. Verificare la configurazione dopo il riavvio:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type          Summary
-----
-----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0          1500 100M up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
    eth0
IP Address: fd20:8ble:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
    lo
IP Address: ::1/128
+ swp1s0        9216 10G      up cluster01          e0b
swp
.
.
.
+ swp15         9216 100G      up sw2                  swp15
swp
+ swp16         9216 100G      up sw2                  swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                        operational  applied  description
-----
enable                on           Turn feature 'on' or
'off'. This feature is disabled by default.
mode                  lossless   lossless  Roce Mode
congestion-control
    congestion-mode    ECN,RED    Congestion config mode
    enabled-tc         0,2,5      Congestion config enabled
Traffic Class
    max-threshold      195.31 KB  Congestion config max-
threshold
    min-threshold      39.06 KB   Congestion config min-
threshold
    probability        100
lldp-app-tlv
    priority           3          switch-priority of roce
    protocol-id        4791       L4 port number
    selector           UDP          L4 protocol
pfc
    pfc-priority       2, 5       switch-prio on which PFC
is enabled
    rx-enabled         enabled      PFC Rx Enabled status
    tx-enabled         enabled      PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations

```
=====
```

	pcp	dscp	switch-prio
--	---	-----	-----
0	0	0,1,2,3,4,5,6,7	0
1	1	8,9,10,11,12,13,14,15	1
2	2	16,17,18,19,20,21,22,23	2
3	3	24,25,26,27,28,29,30,31	3
4	4	32,33,34,35,36,37,38,39	4
5	5	40,41,42,43,44,45,46,47	5
6	6	48,49,50,51,52,53,54,55	6
7	7	56,57,58,59,60,61,62,63	7

RoCE SP->TC mapping and ETS configurations

```
=====
```

	switch-prio	traffic-class	scheduler-weight
--	-----	-----	-----
0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

```
=====
```

	name	mode	size	switch-priorities	
traffic-class					
--	-----	-----	----	-----	
0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7	-
1	roce-reserved-ingress	Dynamic	50%	2,5	-
2	lossy-default-egress	Dynamic	50%	-	0
3	roce-reserved-egress	Dynamic	inf	-	2,5

Exception List

```
=====
```

description
--


```

1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link

```

fast-linkup

Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link fast-linkup



Le eccezioni elencate non influiscono sulle prestazioni e possono essere ignorate senza problemi.

6. Verificare le informazioni per il ricetrasmittitore nell'interfaccia:

```
admin@sw1:mgmt:~$ nv show interface --view=pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor
SN	Vendor Rev			
-----	-----	-----	-----	
swp1s0	0x00 None			
swp1s1	0x00 None			
swp1s2	0x00 None			
swp1s3	0x00 None			
swp2s0	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s1	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s2	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s3	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp3	0x00 None			
swp4	0x00 None			
swp5	0x00 None			
swp6	0x00 None			
.				
.				
.				
swp15	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210117	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210166	B0			

7. Verificare che ciascun nodo abbia una connessione con ciascun switch:

```
admin@sw1:mgmt:~$ nv show interface --view=lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
eth0	100M	Mgmt	mgmt-sw1	Eth110/1/29
swp2s1	25G	Trunk/L2	node1	e0a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

8. 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:

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

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

b. Verificare lo stato di integrità dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono posizionati su e0d).

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

Node/	Local	Discovered			
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform	

node1/lldp					
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-	
node2/lldp					
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-	

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

Switch	Type	Address
Model		

sw1	cluster-network	10.233.205.90
MSN2100-CB2RC		
Serial Number: MNXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 5.4.0 running on		
Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		
sw2	cluster-network	10.233.205.91
MSN2100-CB2RC		
Serial Number: MNCXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 5.4.0 running on		
Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		

9. Verificare che il cluster sia integro:

```
cluster show
```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.

11. Abilita il ripristino automatico sui LIF del cluster.

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

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare il ping comando per verificare la connettività al server che ospita Cumulus Linux e RCF.
3. Visualizza le porte del cluster su ciascun nodo connesso agli switch del cluster:

```
network device-discovery show
```

4. 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 -role cluster
```

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

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

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

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

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
```

- Se stai aggiornando il tuo RCF, devi disabilitare il ripristino automatico per questo passaggio.
- Se hai appena aggiornato la tua versione di Cumulus Linux, non è necessario disattivare il ripristino automatico per questo passaggio perché è già disattivato.

1. Visualizza le interfacce disponibili sullo switch SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216   200G   up
bond
+ eth0          1500   100M   up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216   10G    up    cluster01         e0b
swp
.
.
.
+ swp15         9216   100G    up    sw2                swp15
swp
+ swp16         9216   100G    up    sw2                swp16
swp
```

2. Copiare lo script RCF Python sullo switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



Sebbene `scp` viene utilizzato nell'esempio, puoi usare il tuo metodo preferito per il trasferimento dei file, ad esempio SFTP, HTTPS o FTP.

3. Applicare lo script python RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA  
-Breakout-LLDP  
[sudo] password for cumulus:  
.  
.  
Step 1: Creating the banner file  
Step 2: Registering banner message  
Step 3: Updating the MOTD file  
Step 4: Ensuring passwordless use of cl-support command by admin  
Step 5: Disabling apt-get  
Step 6: Creating the interfaces  
Step 7: Adding the interface config  
Step 8: Disabling cdp  
Step 9: Adding the lldp config  
Step 10: Adding the RoCE base config  
Step 11: Modifying RoCE Config  
Step 12: Configure SNMP  
Step 13: Reboot the switch
```

Lo script RCF completa i passaggi elencati nell'esempio precedente.



Nel passaggio 3 **Aggiornamento del file MOTD** sopra riportato, viene eseguito il comando `cat /etc/issue.net`. Ciò consente di verificare il nome del file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.

Per esempio:

```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1       : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2       : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



Per qualsiasi problema relativo allo script python RCF che non può essere corretto, contattare ["Supporto NetApp"](#) per assistenza.

4. 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.
5. Verificare la configurazione dopo il riavvio:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
-----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0          1500 100M up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
    eth0
IP Address: fd20:8ble:f6ff:fe31:4a0e/64
+ lo            65536      up
loopback      IP Address: 127.0.0.1/8
    lo
IP Address: ::1/128
+ swp1s0        9216 10G      up cluster01          e0b
swp
.
.
.
+ swp15         9216 100G      up sw2                  swp15
swp
+ swp16         9216 100G      up sw2                  swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                        operational  applied  description
-----
enable                  on          Turn feature 'on' or
'off'. This feature is disabled by default.
mode                    lossless   lossless  Roce Mode
congestion-control
    congestion-mode      ECN,RED    Congestion config mode
    enabled-tc           0,2,5     Congestion config enabled
Traffic Class
    max-threshold        195.31 KB Congestion config max-
threshold
    min-threshold        39.06 KB  Congestion config min-
threshold
    probability          100
lldp-app-tlv
    priority             3         switch-priority of roce
    protocol-id          4791      L4 port number
    selector             UDP         L4 protocol
pfc
    pfc-priority         2, 5      switch-prio on which PFC
is enabled
    rx-enabled           enabled    PFC Rx Enabled status
    tx-enabled           enabled    PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations

=====			
	pcp	dscp	switch-prio
--	---	-----	-----
0	0	0,1,2,3,4,5,6,7	0
1	1	8,9,10,11,12,13,14,15	1
2	2	16,17,18,19,20,21,22,23	2
3	3	24,25,26,27,28,29,30,31	3
4	4	32,33,34,35,36,37,38,39	4
5	5	40,41,42,43,44,45,46,47	5
6	6	48,49,50,51,52,53,54,55	6
7	7	56,57,58,59,60,61,62,63	7

RoCE SP->TC mapping and ETS configurations

=====			
	switch-prio	traffic-class	scheduler-weight
--	-----	-----	-----
0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

=====						
name		mode	size	switch-priorities		
traffic-class						
--	-----	-----	----	-----		

0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7		-
1	roce-reserved-ingress	Dynamic	50%	2,5		-
2	lossy-default-egress	Dynamic	50%	-		0
3	roce-reserved-egress	Dynamic	inf	-		2,5

Exception List

=====	
	description
--	-----
---	...

```

1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
    1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
    Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
    Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
    Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
    Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
    Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
    Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
    Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
    Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link

```

fast-linkup

Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link fast-linkup



Le eccezioni elencate non influiscono sulle prestazioni e possono essere ignorate senza problemi.

6. Verificare le informazioni per il ricetrasmittitore nell'interfaccia:

```
admin@sw1:mgmt:~$ nv show platform transceiver
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor
SN	Vendor Rev			
-----	-----	-----	-----	
swp1s0	0x00 None			
swp1s1	0x00 None			
swp1s2	0x00 None			
swp1s3	0x00 None			
swp2s0	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s1	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s2	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s3	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp3	0x00 None			
swp4	0x00 None			
swp5	0x00 None			
swp6	0x00 None			
.				
.				
.				
swp15	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210117	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210166	B0			

7. Verificare che ciascun nodo abbia una connessione con ciascun switch:

```
admin@sw1:mgmt:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
eth0	100M	Mgmt	mgmt-sw1	Eth110/1/29
swp2s1	25G	Trunk/L2	node1	e0a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

8. 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:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

b. Verificare lo stato di integrità dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono posizionati su e0d).

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

Node/	Local	Discovered			
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform	

node1/lldp					
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-	
node2/lldp					
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-	

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

Switch	Type	Address
Model		

sw1	cluster-network	10.233.205.90
MSN2100-CB2RC		
Serial Number: MNXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 5.4.0 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		
sw2	cluster-network	10.233.205.91
MSN2100-CB2RC		
Serial Number: MNCXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 5.4.0 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		

9. Verificare che il cluster sia integro:

```
cluster show
```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.

11. Abilita il ripristino automatico sui LIF del cluster.

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

Cosa succederà ora?

Dopo aver installato l'RCF, puoi ["installare il file CSHM"](#).

Installare il file di configurazione di Ethernet Switch Health Monitor

Per configurare il monitoraggio dello stato dello switch Ethernet sugli switch Ethernet NVIDIA , seguire questa procedura.

Queste istruzioni si applicano se gli switch NVIDIA X190006-PE e X190006-PI non vengono rilevati correttamente, il che può essere confermato eseguendo `system switch ethernet show` e controlla se per il tuo modello viene visualizzato **ALTRO**. Per identificare il modello del tuo switch NVIDIA , trova il numero di parte con il comando `nv show platform hardware` per NVIDIA CL 5.8 e precedenti o `nv show platform` per le versioni successive.



Questi passaggi sono consigliati anche se si desidera che il monitoraggio dello stato e la raccolta dei registri funzionino come previsto quando si utilizza NVIDIA CL 5.11.x con le seguenti versioni ONTAP . Anche se il monitoraggio dello stato di salute e la raccolta dei registri potrebbero funzionare anche senza questi passaggi, seguirli garantisce che tutto funzioni correttamente.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 e versioni successive

Prima di iniziare

- Assicurarsi che il cluster ONTAP sia attivo e funzionante.
- Abilitare SSH sullo switch per utilizzare tutte le funzionalità disponibili in CSHM.
- Cancella il `/mroot/etc/cshm_nod/nod_sign/` directory su tutti i nodi:
 - a. Entra nel nodeshell:

```
system node run -node <name>
```
 - b. Passa ai privilegi avanzati:

```
priv set advanced
```
 - c. Elenca i file di configurazione in `/etc/cshm_nod/nod_sign` elenco. Se la directory esiste e contiene file di configurazione, elenca i nomi dei file.

```
ls /etc/cshm_nod/nod_sign
```
 - d. Elimina tutti i file di configurazione corrispondenti ai modelli di switch connessi.

In caso di dubbi, rimuovere tutti i file di configurazione per i modelli supportati elencati sopra, quindi scaricare e installare i file di configurazione più recenti per quegli stessi modelli.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Verificare che i file di configurazione eliminati non siano più presenti nella directory:

```
ls /etc/cshm_nod/nod_sign
```

Passi

1. Scaricare il file zip di configurazione del monitoraggio dello stato dello switch Ethernet in base alla versione di rilascio ONTAP corrispondente. Questo file è disponibile presso ["Switch Ethernet NVIDIA"](#) pagina.
 - a. Nella pagina di download del software NVIDIA SN2100, seleziona **File Nvidia CSHM**.
 - b. Nella pagina Attenzione/Da leggere assolutamente, seleziona la casella di controllo per accettare.
 - c. Nella pagina del Contratto di licenza con l'utente finale, seleziona la casella di controllo per accettare e fai clic su **Accetta e continua**.
 - d. Nella pagina Nvidia CSHM File - Download, seleziona il file di configurazione applicabile. Sono disponibili i seguenti file:

ONTAP 9.15.1 e versioni successive

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 attraverso 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Carica il file zip applicabile sul tuo server web interno.
2. Accedere all'impostazione della modalità avanzata da uno dei sistemi ONTAP nel cluster.

```
set -privilege advanced
```

3. Eseguire il comando di configurazione del monitor di integrità dello switch.

```
cluster1::> system switch ethernet configure-health-monitor
```

4. Verificare che l'output del comando termini con il seguente testo per la versione ONTAP :

ONTAP 9.15.1 e versioni successive

Il monitoraggio dello stato dello switch Ethernet ha installato il file di configurazione.

ONTAP 9.11.1 attraverso 9.14.1

SHM ha installato il file di configurazione.

ONTAP 9.10.1

Pacchetto scaricato CSHM elaborato correttamente.

Se si verifica un errore, contattare l'assistenza NetApp .

1. Attendi fino al doppio dell'intervallo di polling del monitor di integrità dello switch Ethernet, rilevato eseguendo `system switch ethernet polling-interval show` , prima di completare il passaggio successivo.
2. Esegui il comando `system switch ethernet configure-health-monitor show` sul sistema ONTAP e assicurarsi che gli switch del cluster vengano rilevati con il campo monitorato impostato su **True** e che il campo del numero di serie non mostri **Unknown**.

```
cluster1::> system switch ethernet configure-health-monitor show
```



Se il modello continua a visualizzare **OTHER** dopo aver applicato il file di configurazione, contattare l'assistenza NetApp .

Vedi il "[switch di sistema ethernet configura-monitor-stato](#)" comando per ulteriori dettagli.

Cosa succederà ora?

Dopo aver installato il file CSHM, puoi "[configurare il monitoraggio dello stato dello switch](#)" .

Ripristinare lo switch del cluster SN2100 ai valori predefiniti di fabbrica

Per ripristinare le impostazioni predefinite di fabbrica dello switch cluster SN2100:

- Per Cumulus Linux 5.10 e versioni precedenti, applicare l'immagine Cumulus.
- Per Cumulus Linux 5.11 e versioni successive, utilizzare `nv action reset system factory-default` comando.

Informazioni su questo compito

- È necessario connettersi allo switch tramite la console seriale.
- Per accedere ai comandi tramite sudo è necessario disporre della password di root.



Per ulteriori informazioni sull'installazione di Cumulus Linux, vedere "[Flusso di lavoro di installazione del software per gli switch NVIDIA SN2100](#)" .

Esempio 5. Passi

Cumulus Linux 5.10 e versioni precedenti

1. Dalla console Cumulus, scarica e metti in coda l'installazione del software dello switch con il comando `onie-install -a -i` seguito dal percorso del file al software di commutazione, ad esempio:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. Il programma di installazione avvia il download. Digitare **y** quando richiesto per confermare l'installazione quando l'immagine è stata scaricata e verificata.
3. Riavviare lo switch per installare il nuovo software.

```
sudo reboot
```

```
cumulus@sw1:mgmt:~$ sudo reboot
```



Lo switch si riavvia e avvia l'installazione del software, operazione che richiede un po' di tempo. Una volta completata l'installazione, lo switch si riavvia e rimane allo stato `log-in` richiesta.

Cumulus Linux 5.11 e versioni successive

1. Per ripristinare le impostazioni predefinite di fabbrica dello switch e rimuovere tutti i file di configurazione, di sistema e di registro, eseguire:

```
nv action reset system factory-default
```

Per esempio:

```
cumulus@switch:~$ nv action reset system factory-default
```

```
This operation will reset the system configuration, delete the log files and reboot the switch.
```

```
Type [y] continue.
```

```
Type [n] to abort.
```

```
Do you want to continue? [y/n] y
```

Vedi NVIDIA ["Ripristino delle impostazioni di fabbrica"](#) documentazione per ulteriori dettagli.

Cosa c'è dopo?

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

Migrare gli switch

Migrazione degli switch cluster CN1610 agli switch cluster NVIDIA SN2100

È possibile migrare gli switch cluster NetApp CN1610 per un cluster ONTAP verso gli switch cluster NVIDIA SN2100. Si tratta di una procedura non distruttiva.

Requisiti di revisione

Quando si sostituiscono gli switch cluster NetApp CN1610 con gli switch cluster NVIDIA SN2100, è necessario conoscere alcune informazioni sulla configurazione, sulle connessioni delle porte e sui requisiti di cablaggio. Vedere ["Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100"](#).

Switch supportati

Sono supportati i seguenti switch cluster:

- NetApp CN1610
- NVIDIA SN2100

Per i dettagli sulle porte supportate e le relative configurazioni, vedere ["Hardware Universe"](#).

Prima di iniziare

Verifica di soddisfare i seguenti requisiti per la tua configurazione:

- Il cluster esistente è configurato e funzionante correttamente.
- Tutte le porte del cluster sono nello stato **attivo** per garantire operazioni senza interruzioni.
- Gli switch cluster NVIDIA SN2100 sono configurati e funzionano con la versione corretta di Cumulus Linux installata con il file di configurazione di riferimento (RCF) applicato.
- La configurazione di rete del cluster esistente è la seguente:
 - Un cluster NetApp ridondante e completamente funzionale che utilizza switch CN1610.
 - Connettività di gestione e accesso alla console sia per gli switch CN1610 che per i nuovi switch.
 - Tutti i cluster LIF sono attivi con i cluster LIF sulle rispettive porte home.
 - Porte ISL abilitate e cablate tra gli switch CN1610 e tra i nuovi switch.
- Alcune porte sono configurate sugli switch NVIDIA SN2100 per funzionare a 40GbE o 100GbE.
- Hai pianificato, migrato e documentato la connettività 40GbE e 100GbE dai nodi agli switch cluster NVIDIA SN2100.

Migrare gli switch

Informazioni sugli esempi

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

- Gli switch cluster CN1610 esistenti sono *c1* e *c2*.
- I nuovi switch cluster NVIDIA SN2100 sono *sw1* e *sw2*.
- I nodi sono *node1* e *node2*.
- I LIF del cluster sono *node1_clus1* e *node1_clus2* sul nodo 1, e *node2_clus1* e *node2_clus2* sul nodo 2, rispettivamente.

- IL `cluster1: :*>` il prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono *e3a* e *e3b*.
- Le porte breakout hanno il formato: `swp[porta]s[porta breakout 0-3]`. Ad esempio, quattro porte breakout su `swp1` sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Informazioni su questo compito

Questa procedura copre il seguente scenario:

- Lo switch `c2` viene sostituito prima dallo switch `sw2`.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Il cablaggio tra i nodi e `c2` viene quindi scollegato da `c2` e ricollegato a `sw2`.
- L'interruttore `c1` è sostituito dall'interruttore `sw1`.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Il cablaggio tra i nodi e `c1` viene quindi scollegato da `c1` e ricollegato a `sw1`.



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.

Fase 1: Prepararsi alla migrazione

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.

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (`*>`).

3. Disabilitare il ripristino automatico sui LIF del cluster:

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

Passaggio 2: configurare porte e cablaggio

1. Determinare lo stato amministrativo o operativo per ciascuna interfaccia del cluster.

Ogni porta dovrebbe essere visualizzata per `Link E healthy per Health Status`.

- a. Visualizza gli attributi della porta di rete:

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

Mostra esempio

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Visualizza informazioni sui LIF e sui nodi domestici designati:

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

Ogni LIF dovrebbe visualizzare up/up per Status Admin/Oper E true per Is Home .

Mostra esempio

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

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

Cluster					
e3a		node1_clus1	up/up	169.254.209.69/16	node1
	true				
e3b		node1_clus2	up/up	169.254.49.125/16	node1
	true				
e3a		node2_clus1	up/up	169.254.47.194/16	node2
	true				
e3b		node2_clus2	up/up	169.254.19.183/16	node2
	true				

2. Le porte del cluster su ciascun nodo vengono collegate agli switch del cluster esistenti nel modo seguente (dal punto di vista dei nodi) utilizzando il comando:

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

Mostra esempio

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/cdp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/1	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	0/1	-
node2	/cdp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/2	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	0/2	-

3. Le porte e gli switch del cluster vengono collegati nel modo seguente (dal punto di vista degli switch) utilizzando il comando:

```
show cdp neighbors
```

Mostra esempio



```
c1# 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 e3a	0/1	124	H	AFF-A400
node2 e3a	0/2	124	H	AFF-A400
c2 0/13	0/13	179	S I s	CN1610
c2 0/14	0/14	175	S I s	CN1610
c2 0/15	0/15	179	S I s	CN1610
c2 0/16	0/16	175	S I s	CN1610

```
c2# 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 e3b	0/1	124	H	AFF-A400
node2 e3b	0/2	124	H	AFF-A400
c1 0/13	0/13	175	S I s	CN1610
c1 0/14	0/14	175	S I s	CN1610
c1 0/15	0/15	175	S I s	CN1610
c1 0/16	0/16	175	S I s	CN1610

4. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
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. Sullo switch c2, chiudere le porte connesse alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.

```

(c2)# configure
(c2)(Config)# interface 0/1-0/12
(c2)(Interface 0/1-0/12)# shutdown
(c2)(Interface 0/1-0/12)# exit
(c2)(Config)# exit
(c2)#

```

2. Spostare le porte del cluster di nodi dal vecchio switch c2 al nuovo switch sw2, utilizzando un cablaggio appropriato supportato da NVIDIA SN2100.
3. Visualizza gli attributi della porta di rete:

```

network port show -ipspace Cluster

```

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1	/lldp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/1	-
	e3b	sw2 (b8:ce:f6:19:1a:7e)	swp3	-
node2	/lldp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/2	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

5. Sullo switch sw2, verificare che tutte le porte del cluster dei nodi siano attive:

```
net show interface
```

Mostra esempio

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

6. Sullo switch c1, chiudere le porte collegate alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.

```
(c1)# configure
(c1)(Config)# interface 0/1-0/12
(c1)(Interface 0/1-0/12)# shutdown
(c1)(Interface 0/1-0/12)# exit
(c1)(Config)# exit
(c1)#
```

7. Spostare le porte del cluster di nodi dal vecchio switch c1 al nuovo switch sw1, utilizzando un cablaggio appropriato supportato da NVIDIA SN2100.
8. Verificare la configurazione finale del cluster:

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

Ogni porta dovrebbe visualizzare up per Link E healthy per Health Status .

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

9. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

10. Sugli switch sw1 e sw2, verificare che tutte le porte del cluster di nodi siano attive:

```
net show interface
```

Mostra esempio

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw2 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw2 (swp16)
Master: cluster_isl(UP)					

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

11. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
net show lldp
```

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster:

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

2. Sullo switch sw2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle loro porte home.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. Verificare che i LIF del cluster siano tornati alle loro porte home (potrebbe volerci un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

3. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Migrazione da uno switch cluster Cisco a uno switch cluster NVIDIA SN2100

È possibile migrare gli switch cluster Cisco per un cluster ONTAP verso gli switch cluster NVIDIA SN2100. Si tratta di una procedura non distruttiva.

Requisiti di revisione

Quando si sostituiscono alcuni vecchi switch cluster Cisco con switch cluster NVIDIA SN2100, è necessario conoscere alcune informazioni sulla configurazione, sui collegamenti delle porte e sui requisiti di cablaggio. Vedere ["Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100"](#).

Switch supportati

Sono supportati i seguenti switch cluster Cisco :

- Nexus 9336C-FX2
- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Per i dettagli sulle porte supportate e le relative configurazioni, vedere ["Hardware Universe"](#).

Cosa ti servirà

Assicurarsi che:

- Il cluster esistente è configurato e funzionante correttamente.
- Tutte le porte del cluster sono nello stato **attivo** per garantire operazioni senza interruzioni.
- Gli switch cluster NVIDIA SN2100 sono configurati e funzionano con la versione corretta di Cumulus Linux installata con il file di configurazione di riferimento (RCF) applicato.
- La configurazione di rete del cluster esistente presenta quanto segue:
 - Un cluster NetApp ridondante e completamente funzionale che utilizza entrambi gli switch Cisco più vecchi.
 - Connettività di gestione e accesso alla console sia per i vecchi switch Cisco sia per quelli nuovi.
 - Tutti i cluster LIF nello stato attivo con i cluster LIF sulle loro porte home.
 - Porte ISL abilitate e cablate tra i vecchi switch Cisco e tra i nuovi switch.
- Alcune porte sono configurate sugli switch NVIDIA SN2100 per funzionare a 40 GbE o 100 GbE.
- Hai pianificato, migrato e documentato la connettività 40 GbE e 100 GbE dai nodi agli switch cluster NVIDIA SN2100.



Se si modifica la velocità delle porte cluster e0a ed e1a sui sistemi AFF A800 o AFF C800 , è possibile che vengano ricevuti pacchetti malformati dopo la conversione della velocità. Vedere ["Errore 1570339"](#) e l'articolo della Knowledge Base ["Errori CRC sulle porte T6 dopo la conversione da 40 GbE a 100 GbE"](#) per avere una guida.

Migrare gli switch

Informazioni sugli esempi

In questa procedura, per i comandi e gli output di esempio vengono utilizzati gli switch cluster Cisco Nexus 3232C.

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

- Gli switch cluster Cisco Nexus 3232C esistenti sono *c1* e *c2*.
- I nuovi switch cluster NVIDIA SN2100 sono *sw1* e *sw2*.
- I nodi sono *node1* e *node2*.
- I LIF del cluster sono *node1_clus1* e *node1_clus2* sul nodo 1, e *node2_clus1* e *node2_clus2* sul nodo 2, rispettivamente.
- IL `cluster1::*>` il prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono *e3a* e *e3b*.
- Le porte breakout hanno il formato: `swp[porta]s[porta breakout 0-3]`. Ad esempio, quattro porte breakout su *swp1* sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Informazioni su questo compito

Questa procedura copre il seguente scenario:

- Lo switch *c2* viene sostituito prima dallo switch *sw2*.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Il cablaggio tra i nodi e *c2* viene quindi scollegato da *c2* e ricollegato a *sw2*.
- L'interruttore *c1* è sostituito dall'interruttore *sw1*.
 - Chiudere le porte verso i nodi del cluster. Per evitare l'instabilità del cluster, tutte le porte devono essere chiuse contemporaneamente.
 - Il cablaggio tra i nodi e *c1* viene quindi scollegato da *c1* e ricollegato a *sw1*.

Fase 1: Prepararsi alla migrazione

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.

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

3. Disabilitare il ripristino automatico sui LIF del cluster:

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

Passaggio 2: configurare porte e cablaggio

1. Determinare lo stato amministrativo o operativo per ciascuna interfaccia del cluster.

Ogni porta dovrebbe essere visualizzata per `Link` e `sano` per `Health Status`.

- a. Visualizza gli attributi della porta di rete:

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

Mostra esempio

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

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Visualizza informazioni sulle interfacce logiche e sui nodi home designati:

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

Ogni LIF dovrebbe visualizzare up/up per Status Admin/Oper e vero per Is Home .

Mostra esempio

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

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

Cluster					
		node1_clus1	up/up	169.254.209.69/16	node1
e3a	true				
		node1_clus2	up/up	169.254.49.125/16	node1
e3b	true				
		node2_clus1	up/up	169.254.47.194/16	node2
e3a	true				
		node2_clus2	up/up	169.254.19.183/16	node2
e3b	true				

2. Le porte del cluster su ciascun nodo sono collegate agli switch del cluster esistenti nel modo seguente (dal punto di vista dei nodi):

```
network device-discovery show -protocol lldp
```

Mostra esempio

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/lldp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	Eth1/1	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	Eth1/1	-
node2	/lldp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	Eth1/2	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	Eth1/2	-

3. Le porte e gli switch del cluster sono collegati nel modo seguente (dal punto di vista degli switch):

```
show cdp neighbors
```

Mostra esempio

```
c1# 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 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
c2 Eth1/31	Eth1/31	179	S I s	N3K-C3232C
c2 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

```
c2# 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 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
c1 Eth1/31	Eth1/31	175	S I s	N3K-C3232C
c1 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

4. 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	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
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. Sullo switch c2, spegnere le porte connesse alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.

```

(c2)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2) (Config)# interface
(c2) (config-if-range)# shutdown <interface_list>
(c2) (config-if-range)# exit
(c2) (Config)# exit
(c2)#

```

2. Spostare le porte del cluster di nodi dal vecchio switch c2 al nuovo switch sw2, utilizzando un cablaggio appropriato supportato da NVIDIA SN2100.
3. Visualizza gli attributi della porta di rete:

```

network port show -ipspace Cluster

```

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

Mostra esempio

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
-----	-----	-----	-----
node1	/lldp		
	e3a	c1 (6a:ad:4f:98:3b:3f)	Eth1/1 -
	e3b	sw2 (b8:ce:f6:19:1a:7e)	swp3 -
node2	/lldp		
	e3a	c1 (6a:ad:4f:98:3b:3f)	Eth1/2 -
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4 -

5. Sullo switch sw2, verificare che tutte le porte del cluster dei nodi siano attive:

```
net show interface
```

Mostra esempio

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					
-----	-----	-----	-----	-----	-----
...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

6. Sullo switch c1, chiudere le porte collegate alle porte del cluster dei nodi per eseguire il failover dei LIF del cluster.

```
(c1)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1) (Config)# interface
(c1) (config-if-range)# shutdown <interface_list>
(c1) (config-if-range)# exit
(c1) (Config)# exit
(c1)#
```

7. Spostare le porte del cluster di nodi dal vecchio switch c1 al nuovo switch sw1, utilizzando un cablaggio appropriato supportato da NVIDIA SN2100.
8. Verificare la configurazione finale del cluster:

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

Ogni porta dovrebbe visualizzare up per Link e sano per Health Status .

Mostra esempio

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

9. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
-----	-----	-----	-----	
node1	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

10. Sugli switch sw1 e sw2, verificare che tutte le porte del cluster di nodi siano attive:

```
net show interface
```

Mostra esempio

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw2 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw2 (swp16)
Master: cluster_isl(UP)					

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

11. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
net show lldp
```

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico sui LIF del cluster:

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

2. Sullo switch sw2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle loro porte home.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. Verificare che i LIF del cluster siano tornati alle loro porte home (potrebbe volerci un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

3. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Migrare a un cluster commutato a due nodi con switch cluster NVIDIA SN2100

Se disponi di un ambiente cluster switchless a due nodi esistente, puoi migrare a un ambiente cluster switched a due nodi utilizzando gli switch NVIDIA SN2100 per poter scalare oltre due nodi nel cluster.

La procedura da utilizzare varia a seconda che si disponga di due porte di rete cluster dedicate su ciascun controller o di una singola porta cluster su ciascun controller. Il processo documentato funziona per tutti i nodi che utilizzano porte ottiche o Twinax, ma non è supportato su questo switch se i nodi utilizzano porte RJ45 10GBASE-T integrate per le porte della rete cluster.

Requisiti di revisione

Configurazione switchless a due nodi

Assicurarsi che:

- La configurazione switchless a due nodi è correttamente configurata e funzionante.
- I nodi eseguono ONTAP 9.10.1P3 e versioni successive.
- Tutte le porte del cluster sono nello stato **attivo**.
- Tutte le interfacce logiche del cluster (LIF) sono nello stato **attivo** e sulle loro porte home.

Configurazione dello switch cluster NVIDIA SN2100

Assicurarsi che:

- Entrambi gli switch dispongono di connettività di rete di gestione.
- È disponibile l'accesso alla console per gli switch del cluster.
- Le connessioni tra switch e nodi NVIDIA SN2100 utilizzano cavi Twinax o in fibra.



Vedere ["Esaminare le considerazioni sul cablaggio e sulla configurazione"](#) per avvertenze e ulteriori dettagli. IL ["Hardware Universe - Interruttori"](#) contiene anche maggiori informazioni sul cablaggio.

- I cavi Inter-Switch Link (ISL) sono collegati alle porte swp15 e swp16 su entrambi gli switch NVIDIA SN2100.
- La personalizzazione iniziale di entrambi gli switch SN2100 è stata completata, in modo che:
 - Gli switch SN2100 eseguono l'ultima versione di Cumulus Linux
 - I file di configurazione di riferimento (RCF) vengono applicati agli switch
 - Sui nuovi switch vengono configurate tutte le personalizzazioni del sito, come SMTP, SNMP e SSH.

IL ["Hardware Universe"](#) contiene le informazioni più recenti sulle porte cluster effettive per le tue piattaforme.

Migrare gli switch

Informazioni sugli esempi

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

- I nomi degli switch SN2100 sono *sw1* e *sw2*.
- I nomi degli SVM del cluster sono *node1* e *node2*.
- I nomi dei LIF sono *node1_clus1* e *node1_clus2* sul nodo 1, e *node2_clus1* e *node2_clus2* sul nodo 2, rispettivamente.
- IL `cluster1: :*>` il prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono *e3a* e *e3b*.
- Le porte breakout hanno il formato: `swp[porta]s[porta breakout 0-3]`. Ad esempio, quattro porte breakout su *swp1* sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Fase 1: Prepararsi alla migrazione

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.

2. Cambia il livello di privilegio in avanzato, inserendo *y* quando viene richiesto di continuare: `set -privilege advanced`

Il prompt avanzato(**>*) appare.

Passaggio 2: configurare porte e cablaggio

Cumulus Linux 4.4.x

1. Disabilitare tutte le porte rivolte verso il nodo (non le porte ISL) su entrambi i nuovi switch cluster sw1 e sw2.

Non è consentito disattivare le porte ISL.

I seguenti comandi disabilitano le porte rivolte al nodo sugli switch sw1 e sw2:

```
cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit

cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

2. Verificare che l'ISL e le porte fisiche sull'ISL tra i due switch SN2100 sw1 e sw2 siano attive sulle porte swp15 e swp16:

```
net show interface
```

I seguenti comandi mostrano che le porte ISL sono attive sugli switch sw1 e sw2:

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp15	100G	9216	BondMember	sw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw2 (swp16)	Master: cluster_isl (UP)

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master: cluster_isl (UP)

Cumulus Linux 5.x

1. Disabilitare tutte le porte rivolte verso il nodo (non le porte ISL) su entrambi i nuovi switch cluster sw1 e sw2.

Non è consentito disattivare le porte ISL.

I seguenti comandi disabilitano le porte rivolte al nodo sugli switch sw1 e sw2:

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw1:~$ nv config apply  
cumulus@sw1:~$ nv config save  
  
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv config save
```

2. Verificare che l'ISL e le porte fisiche sull'ISL tra i due switch SN2100 sw1 e sw2 siano attive sulle porte swp15 e swp16:

```
nv show interface
```

Gli esempi seguenti mostrano che le porte ISL sono attive sugli switch sw1 e sw2:

```
cumulus@sw1:~$ nv show interface
```

Interface	MTU	Speed	State	Remote Host	Remote Port
Type	Summary				

...					
...					
+ swp14	9216		down		
swp					
+ swp15	9216	100G	up	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

```
cumulus@sw2:~$ nv show interface
```

Interface	MTU	Speed	State	Remote Host	Remote Port
Type	Summary				

...					
...					
+ swp14	9216		down		
swp					
+ swp15	9216	100G	up	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

1. Verificare che tutte le porte del cluster siano attive:

```
network port show
```

Ogni porta dovrebbe visualizzare up per Link e sano per Health Status .

Mostra esempio

```
cluster1::*> network port show
```

```
Node: node1
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node2
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

2. Verificare che tutti i cluster LIF siano attivi e operativi:

```
network interface show
```

Ogni cluster LIF dovrebbe visualizzare true per Is Home e avere un Status Admin/Oper Di up/up .

Mostra esempio

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e3a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e3a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

3. Disabilitare il ripristino automatico sui LIF del cluster:

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

Mostra esempio

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

Vserver	Logical	
Interface	Auto-revert	

Cluster		
	node1_clus1	false
	node1_clus2	false
	node2_clus1	false
	node2_clus2	false

4. Scollegare il cavo dalla porta e3a del cluster sul nodo 3, quindi collegare e3a alla porta 1 sullo switch sw1 del cluster, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

IL ["Hardware Universe - Interruttori"](#) contiene maggiori informazioni sul cablaggio.

5. Scollegare il cavo dalla porta e3a del cluster sul nodo 4, quindi collegare e3a alla porta 2 sullo switch sw1

del cluster, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

Cumulus Linux 4.4.x

1. Sullo switch sw1, abilitare tutte le porte rivolte verso il nodo.

I seguenti comandi abilitano tutte le porte rivolte verso il nodo sullo switch sw1.

```
cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

2. Sullo switch sw1, verificare che tutte le porte siano attive:

```
net show interface all
```

```
cumulus@sw1:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	-----
...						
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3a)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3a)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

Cumulus Linux 5.x

1. Sullo switch sw1, abilitare tutte le porte rivolte verso il nodo.

I seguenti comandi abilitano tutte le porte rivolte verso il nodo sullo switch sw1.

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
up  
cumulus@sw1:~$ nv config apply  
cumulus@sw1:~$ nv config save
```

2. Sullo switch sw1, verificare che tutte le porte siano attive:

```
nv show interface
```

```
cumulus@sw1:~$ nv show interface
```

Interface	State	Speed	MTU	Type	Remote Host
Remote Port	Summary				
-----	-----	-----	-----	-----	
-----	-----	-----	-----	-----	-----
...					
...					
swp1s0	up	10G	9216	swp	odq-a300-1a
e0a					
swp1s1	up	10G	9216	swp	odq-a300-1b
e0a					
swp1s2	down	10G	9216	swp	
swp1s3	down	10G	9216	swp	
swp2s0	down	25G	9216	swp	
swp2s1	down	25G	9216	swp	
swp2s2	down	25G	9216	swp	
swp2s3	down	25G	9216	swp	
swp3	down		9216	swp	
swp4	down		9216	swp	
...					
...					
swp14	down		9216	swp	
swp15	up	100G	9216	swp	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

1. Verificare che tutte le porte del cluster siano attive:

```
network port show -ipSpace Cluster
```

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono attive su node1 e node2:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

2. Visualizza informazioni sullo stato dei nodi nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

3. Scollegare il cavo dalla porta e3b del cluster sul nodo 3, quindi collegare e3b alla porta 1 sullo switch sw2 del cluster, utilizzando il cablaggio appropriato supportato dagli switch SN2100.
4. Scollegare il cavo dalla porta e3b del cluster sul nodo 4, quindi collegare e3b alla porta 2 sullo switch sw2 del cluster, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

Cumulus Linux 4.4.x

1. Sullo switch sw2, abilitare tutte le porte rivolte verso il nodo.

I seguenti comandi abilitano le porte rivolte verso il nodo sullo switch sw2:

```
cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw2:~$ net pending  
cumulus@sw2:~$ net commit
```

2. Sullo switch sw2, verificare che tutte le porte siano attive:

```
net show interface all
```

```
cumulus@sw2:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	-----
...						
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3b)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3b)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

3. Su entrambi gli switch sw1 e sw2, verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
net show lldp
```

L'esempio seguente mostra i risultati appropriati per entrambi gli switch sw1 e sw2:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Cumulus Linux 5.x

1. Sullo switch sw2, abilitare tutte le porte rivolte verso il nodo.

I seguenti comandi abilitano le porte rivolte verso il nodo sullo switch sw2:

```
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
up  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv config save
```

2. Sullo switch sw2, verificare che tutte le porte siano attive:

```
nv show interface
```

```
cumulus@sw2:~$ nv show interface
```

Interface	State	Speed	MTU	Type	Remote Host
Remote Port	Summary				
-----	-----	-----	-----	-----	-----
...					
...					
swp1s0	up	10G	9216	swp	odq-a300-1a
e0a					
swp1s1	up	10G	9216	swp	odq-a300-1b
e0a					
swp1s2	down	10G	9216	swp	
swp1s3	down	10G	9216	swp	
swp2s0	down	25G	9216	swp	
swp2s1	down	25G	9216	swp	
swp2s2	down	25G	9216	swp	
swp2s3	down	25G	9216	swp	
swp3	down		9216	swp	
swp4	down		9216	swp	
...					
...					
swp14	down		9216	swp	
swp15	up	100G	9216	swp	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

3. Su entrambi gli switch sw1 e sw2, verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
nv show interface --view=lldp
```

Gli esempi seguenti mostrano i risultati appropriati per entrambi gli switch sw1 e sw2:

```
cumulus@sw1:~$ nv show interface --view=lldp
```

Interface	Speed	Type	Remote Host
Remote Port			
-----	-----	-----	-----
...			
...			
swp1s0	10G	swp	odq-a300-1a
e0a			

```

swp1s1      10G      swp      odq-a300-1b
e0a
swp1s2      10G      swp
swp1s3      10G      swp
swp2s0      25G      swp
swp2s1      25G      swp
swp2s2      25G      swp
swp2s3      25G      swp
swp3                swp
swp4                swp
...
...
swp14                swp
swp15      100G      swp      ossg-int-rcf10
swp15
swp16      100G      swp      ossg-int-rcf10
swp16

```

```
cumulus@sw2:~$ nv show interface --view=lldp
```

Interface	Speed	Type	Remote Host
Remote Port			
-----	-----	-----	-----

...			
...			
swp1s0	10G	swp	odq-a300-1a
e0a			
swp1s1	10G	swp	odq-a300-1b
e0a			
swp1s2	10G	swp	
swp1s3	10G	swp	
swp2s0	25G	swp	
swp2s1	25G	swp	
swp2s2	25G	swp	
swp2s3	25G	swp	
swp3		swp	
swp4		swp	
...			
...			
swp14		swp	
swp15	100G	swp	ossg-int-rcf10
swp15			
swp16	100G	swp	ossg-int-rcf10
swp16			

1. Visualizza le informazioni sui dispositivi di rete rilevati nel tuo cluster:

```
network device-discovery show -protocol lldp
```

Mostra esempio

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1      /lldp
           e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3       -
           e3b    sw2 (b8:ce:f6:19:1b:96)   swp3       -
node2      /lldp
           e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4       -
           e3b    sw2 (b8:ce:f6:19:1b:96)   swp4       -
```

2. Verificare che tutte le porte del cluster siano attive:

```
network port show -ipSpace Cluster
```

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono attive su node1 e node2:

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

Node: node1

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Node: node2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Passaggio 3: verificare la configurazione

1. Abilita il ripristino automatico su tutti i LIF del cluster:

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

Mostra esempio

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto  
-revert true
```

Vserver	Logical Interface	Auto-revert
-----	-----	-----
Cluster		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

2. Sullo switch sw2, arrestare e riavviare tutte le porte del cluster per attivare un ripristino automatico di tutti i LIF del cluster che non si trovano sulle loro porte home.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(Wait for 5-10 seconds before re-enabling the ports)

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface
```

(After executing the link state up command, the nodes detect the change and begin to auto-revert the cluster LIFs to their home ports)

1. Verificare che i LIF del cluster siano tornati alle loro porte home (potrebbe volerci un minuto):

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

Se uno qualsiasi dei LIF del cluster non è tornato alla propria porta home, ripristinarlo manualmente. È necessario connettersi a ciascuna console di sistema LIF o SP/ BMC di gestione nodi del nodo locale proprietario del LIF:

```
network interface revert -vserver Cluster -lif *
```

2. Verificare che tutte le interfacce siano visualizzate true per Is Home :

```
net interface show -vserver Cluster
```



Potrebbe volerci un minuto per completare l'operazione.

Mostra esempio

L'esempio seguente mostra che tutti i LIF sono attivi su node1 e node2 e che Is Home i risultati sono veri:

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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e3b
true					

3. Verificare che le impostazioni siano disabilite:

```
network options switchless-cluster show
```

L'output false nell'esempio seguente mostra che le impostazioni di configurazione sono disabilite:

```
cluster1::*> network options switchless-cluster show  
Enable Switchless Cluster: false
```

4. Verificare lo stato dei membri del nodo nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato di integrità e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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. Riporta il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver migrato gli switch, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituire gli interruttori

Sostituire uno switch cluster NVIDIA SN2100

Seguire questa procedura per sostituire uno switch NVIDIA SN2100 difettoso in una rete cluster. Si tratta di una procedura non distruttiva (NDU).

Requisiti di revisione

Cluster esistente e infrastruttura di rete

Assicurarsi che:

- Il cluster esistente è stato verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
- Tutte le porte del cluster sono attive.
- Tutte le interfacce logiche del cluster (LIF) sono attive e sulle rispettive porte home.
- L' `ONTAP cluster ping-cluster -node node1` il comando indica che la connettività di base e la comunicazione più grande di PMTU hanno esito positivo su tutti i percorsi.

Interruttore sostitutivo NVIDIA SN2100

Assicurarsi che:

- La connettività della rete di gestione sullo switch sostitutivo è funzionante.
- L'accesso alla console per l'interruttore sostitutivo è a posto.
- Le connessioni dei nodi sono le porte da swp1 a swp14.
- Tutte le porte Inter-Switch Link (ISL) sono disabilitate sulle porte swp15 e swp16.
- Il file di configurazione di riferimento desiderato (RCF) e lo switch dell'immagine del sistema operativo Cumulus vengono caricati sullo switch.
- La personalizzazione iniziale dello switch è completa.

Assicurarsi inoltre che tutte le personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengano copiate sul nuovo switch.



È necessario eseguire il comando per migrare un cluster LIF dal nodo in cui è ospitato il cluster LIF.

Abilita la registrazione della console

NetApp consiglia vivamente di abilitare la registrazione della console sui dispositivi utilizzati e di adottare le seguenti misure quando si sostituisce lo switch:

- Lasciare AutoSupport abilitato durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione di casi per tutta la durata della manutenzione. Vedi questo articolo della Knowledge Base ["SU92: Come sopprimere la creazione automatica dei casi durante le finestre di manutenzione programmata"](#) per ulteriori dettagli.
- Abilita la registrazione delle sessioni per tutte le sessioni CLI. Per istruzioni su come abilitare la registrazione della sessione, consultare la sezione "Registrazione dell'output della sessione" in questo articolo della Knowledge Base ["Come configurare PuTTY per una connettività ottimale ai sistemi ONTAP"](#).

Sostituire l'interruttore

Informazioni sugli esempi

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

- I nomi degli switch NVIDIA SN2100 esistenti sono *sw1* e *sw2*.
- Il nome del nuovo switch NVIDIA SN2100 è *nsw2*.
- I nomi dei nodi sono *node1* e *node2*.

- Le porte del cluster su ciascun nodo sono denominate *e3a* e *e3b*.
- I nomi LIF del cluster sono *node1_clus1* e *node1_clus2* per *node1*, e *node2_clus1* e *node2_clus2* per *node2*.
- La richiesta di modifiche a tutti i nodi del cluster è `cluster1::*>`
- Le porte breakout hanno il formato: `swp[porta]s[porta breakout 0-3]`. Ad esempio, quattro porte breakout su *swp1* sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Informazioni sulla topologia della rete del cluster

Questa procedura si basa sulla seguente topologia di rete cluster:

Mostra topologia di esempio

cluster1::*> network port show -ipspace Cluster

Node: node1

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

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

Node: node2

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

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

cluster1::*> network interface show -vserver Cluster

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

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					

```

node2_clus1 up/up 169.254.47.194/16 node2 e3a
true
node2_clus2 up/up 169.254.19.183/16 node2 e3b
true

```

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

Node/	Local	Discovered			
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform	
node1	/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-	
node2	/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-	

+

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw2	e3a
swp4	100G	Trunk/L2	sw2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw1	e3b
swp4	100G	Trunk/L2	sw1	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Fase 1: Preparazione alla sostituzione

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.

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

```
set -privilege advanced
```

Viene visualizzato il prompt avanzato (*>).

3. Installare l'RCF e l'immagine appropriati sullo switch, nsw2, ed effettuare tutti i preparativi necessari sul sito.

Se necessario, verificare, scaricare e installare le versioni appropriate del software RCF e Cumulus per il nuovo switch.

- a. È possibile scaricare il software Cumulus applicabile agli switch del cluster dal sito *NVIDIA Support*. Seguire i passaggi indicati nella pagina Download per scaricare Cumulus Linux per la versione del software ONTAP che si sta installando.
- b. L'RCF appropriato è disponibile presso "[Switch di cluster e storage NVIDIA](#)" pagina. Seguire i passaggi indicati nella pagina Download per scaricare il file RCF corretto per la versione del software ONTAP che si sta installando.

Passaggio 2: configurare porte e cablaggio

Cumulus Linux 4.4.3

1. Sul nuovo switch nsw2, accedi come amministratore e chiudi tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da swp1 a swp14).

I LIF sui nodi del cluster dovrebbero già aver eseguito il failover sull'altra porta del cluster per ciascun nodo.

```
cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

2. Disabilitare il ripristino automatico sui LIF del cluster:

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

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

```
Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: y
```

3. Verificare che il ripristino automatico sia disabilitato in tutti i cluster LIF:

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

4. Chiudere le porte ISL swp15 e swp16 sullo switch SN2100 sw1.

```
cumulus@sw1:~$ net add interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

5. Rimuovere tutti i cavi dallo switch SN2100 sw1, quindi collegarli alle stesse porte sullo switch SN2100 nsw2.
6. Attivare le porte ISL swp15 e swp16 tra gli switch sw1 e nsw2.

I seguenti comandi abilitano le porte ISL swp15 e swp16 sullo switch sw1:

```
cumulus@sw1:~$ net del interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

L'esempio seguente mostra che le porte ISL sono attive sullo switch sw1:

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	nsw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	nsw2 (swp16)	Master: cluster_isl (UP)

L'esempio seguente mostra che le porte ISL sono attive sullo switch nsw2:

```
cumulus@nsw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master: cluster_isl (UP)

7. Verificare che la porta e3b è attivo su tutti i nodi:

```
network port show -ipSpace Cluster
```

L'output dovrebbe essere simile al seguente:

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

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Node/	Local	Discovered			
Protocol	Port	Device	(LLDP: ChassisID)	Interface	Platform

node1	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp3	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp3	-
node2	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp4	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp4	-

9. Verificare che tutte le porte del cluster dei nodi siano attive:

```
net show interface
```

```
cumulus@nsw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

10. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
net show lldp
```

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Abilita il ripristino automatico sui LIF del cluster:

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

12. Sullo switch nsw2, richiamare le porte connesse alle porte di rete dei nodi.

```
cumulus@nsw2:~$ net del interface swp1-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

13. Visualizza informazioni sui nodi in un cluster:

```
cluster show
```

Questo esempio mostra che lo stato di integrità del nodo node1 e node2 in questo cluster è corretto:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	true	true
node2	true	true

14. Verificare che tutte le porte fisiche del cluster siano attive:

```
network port show ipspace Cluster
```

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

Node node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Cumulus Linux 5.x

1. Sul nuovo switch nsw2, accedi come amministratore e chiudi tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da swp1 a swp14).

I LIF sui nodi del cluster dovrebbero già aver eseguito il failover sull'altra porta del cluster per ciascun nodo.

```
cumulus@nsw2:~$ nv set interface swp15-16 link state down
cumulus@nsw2:~$ nv config apply
```

2. Disabilitare il ripristino automatico sui LIF del cluster:

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

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

Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: **y**

3. Verificare che il ripristino automatico sia disabilitato in tutti i cluster LIF:

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

4. Chiudere le porte ISL swp15 e swp16 sullo switch SN2100 sw1.

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

5. Rimuovere tutti i cavi dallo switch SN2100 sw1, quindi collegarli alle stesse porte sullo switch SN2100 nsw2.
6. Attivare le porte ISL swp15 e swp16 tra gli switch sw1 e nsw2.

I seguenti comandi abilitano le porte ISL swp15 e swp16 sullo switch sw1:

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

L'esempio seguente mostra che le porte ISL sono attive sullo switch sw1:

```
cumulus@sw1:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	nsw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	nsw2 (swp16)	Master: cluster_isl (UP)

L'esempio seguente mostra che le porte ISL sono attive sullo switch nsw2:

```
cumulus@nsw2:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master:
	cluster_isl (UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master:
	cluster_isl (UP)					

7. Verificare che la porta e3b è attivo su tutti i nodi:

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

L'output dovrebbe essere simile al seguente:

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

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel modo seguente, dal punto di vista dei nodi:

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

Node/	Local	Discovered			
Protocol	Port	Device	(LLDP: ChassisID)	Interface	Platform

node1	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp3	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp3	-
node2	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp4	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp4	-

9. Verificare che tutte le porte del cluster dei nodi siano attive:

```
nv show interface
```

```
cumulus@nsw2:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

10. Verificare che entrambi i nodi abbiano una connessione a ciascun switch:

```
nv show interface lldp
```

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cumulus@sw1:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Abilita il ripristino automatico sui LIF del cluster:

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

12. Sullo switch nsw2, richiamare le porte connesse alle porte di rete dei nodi.

```
cumulus@nsw2:~$ nv set interface swp1-14 link state up  
cumulus@nsw2:~$ nv config apply
```

13. Visualizza informazioni sui nodi in un cluster:

```
cluster show
```

Questo esempio mostra che lo stato di integrità del nodo node1 e node2 in questo cluster è corretto:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	true	true
node2	true	true

14. Verificare che tutte le porte fisiche del cluster siano attive:

```
network port show ipspace Cluster
```

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

Node node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Passaggio 3: verificare la configurazione

Cumulus Linux 4.4.3

1. Verificare che la rete del cluster sia integra.

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

Cumulus Linux 5.x

1. Verificare che la rete del cluster sia integra.

```
cumulus@sw1:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

1. Ripristina il livello di privilegio su amministratore:

```
set -privilege admin
```

2. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Cosa succederà ora?

Dopo aver sostituito gli interruttori, puoi ["configurare il monitoraggio dello stato dello switch"](#).

Sostituisci gli switch cluster NVIDIA SN2100 con connessioni switchless

È possibile migrare da un cluster con una rete di cluster commutata a uno in cui due nodi sono collegati direttamente per ONTAP 9.3 e versioni successive.

Requisiti di revisione

Linee guida

Rivedere le seguenti linee guida:

- La migrazione a una configurazione cluster switchless a due nodi è un'operazione non distruttiva. La maggior parte dei sistemi ha due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per sistemi con un numero maggiore di porte di interconnessione cluster dedicate su ciascun nodo, ad esempio quattro, sei o otto.
- Non è possibile utilizzare la funzionalità di interconnessione del cluster senza switch con più di due nodi.
- Se si dispone di un cluster a due nodi esistente che utilizza switch di interconnessione cluster ed esegue ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

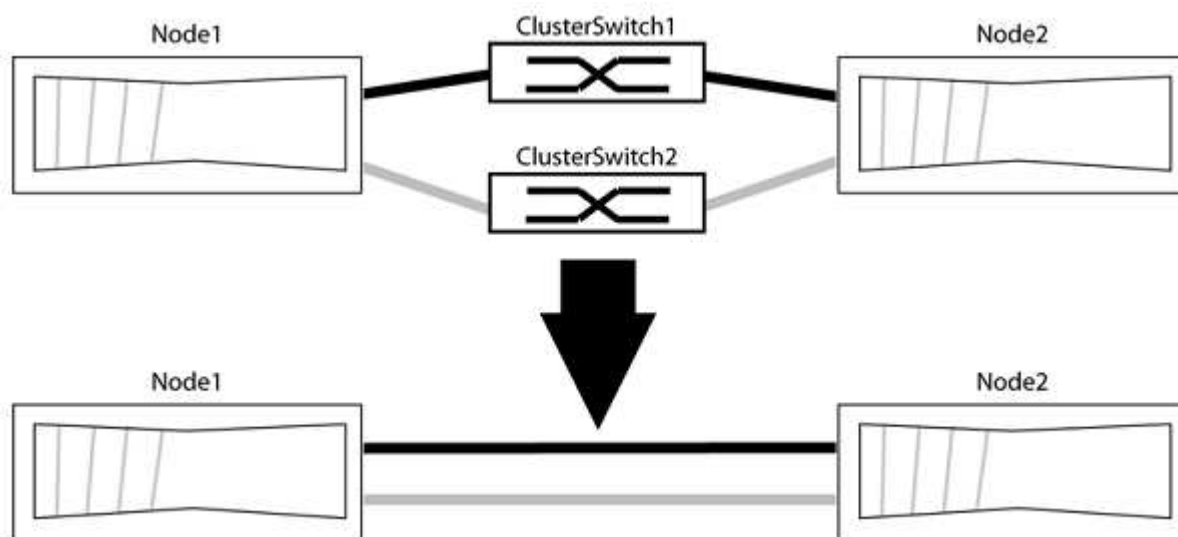
Assicurati di avere quanto segue:

- Un cluster sano costituito da due nodi collegati tramite switch di cluster. I nodi devono eseguire la stessa versione ONTAP .
- Ogni nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, ci sono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

Informazioni su questo compito

La seguente procedura rimuove gli switch del cluster in un cluster a due nodi e sostituisce ogni connessione allo switch con una connessione diretta al nodo partner.



Informazioni sugli esempi

Gli esempi nella seguente procedura mostrano nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse, poiché variano in base al sistema.

Fase 1: Prepararsi alla migrazione

1. Cambia il livello di privilegio in avanzato, inserendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato `*>` appare.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster switchless, abilitato per impostazione predefinita.

È possibile verificare che il rilevamento dei cluster switchless sia abilitato eseguendo il comando con privilegi avanzati:

```
network options detect-switchless-cluster show
```

Mostra esempio

Il seguente output di esempio mostra se l'opzione è abilitata.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Abilita rilevamento cluster senza switch" è `false`, contattare l'assistenza NetApp.

3. 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=<number_of_hours>h
```

Dove `h` è la durata della finestra di manutenzione in ore. Il messaggio avvisa il supporto tecnico di questa attività di manutenzione, in modo che possa sopprimere la creazione automatica dei casi durante la finestra di manutenzione.

Nell'esempio seguente, il comando sopprime la creazione automatica dei casi per due ore:

Mostra esempio

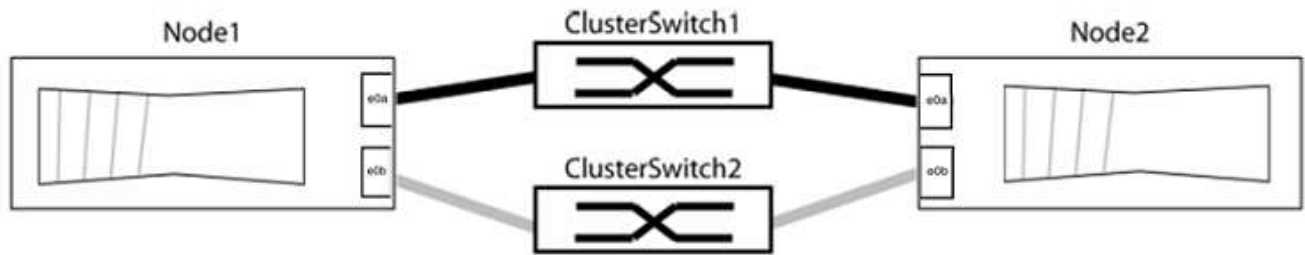
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Passaggio 2: configurare porte e cablaggio

1. Organizzare le porte del cluster su ogni switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano al cluster switch 1 e le porte del cluster nel gruppo 2 vadano al cluster switch 2. Questi gruppi saranno necessari più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e l'integrità del collegamento:

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

Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo è identificato come "nodo1:e0a" e "nodo2:e0a" e l'altro gruppo come "nodo1:e0b" e "nodo2:e0b". I nodi potrebbero utilizzare porte cluster diverse perché variano in base al sistema.



Verificare che le porte abbiano un valore di up per la colonna “Link” e un valore di healthy per la colonna “Stato di salute”.

Mostra esempio

```
cluster::> network port show -ipspace Cluster
```

```
Node: node1
```

```
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: node2
```

```
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
```

```
4 entries were displayed.
```

3. Verificare che tutti i LIF del cluster siano sulle rispettive porte home.

Verificare che la colonna "is-home" sia true per ciascuno dei LIF del cluster:

```
network interface show -vserver Cluster -fields is-home
```

Mostra esempio

```
cluster:*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-----  -
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se sono presenti LIF del cluster che non si trovano sulle loro porte home, ripristinare tali LIF sulle loro porte home:

```
network interface revert -vserver Cluster -lif *
```

4. Disabilitare il ripristino automatico per i LIF del cluster:

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

5. Verificare che tutte le porte elencate nel passaggio precedente siano connesse a uno switch di rete:

```
network device-discovery show -port cluster_port
```

La colonna "Dispositivo rilevato" dovrebbe contenere il nome dello switch del cluster a cui è connessa la porta.

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono collegate correttamente agli switch del cluster "cs1" e "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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 cluster sia integro:

```
cluster ring show
```

Tutte le unità devono essere master o secondarie.

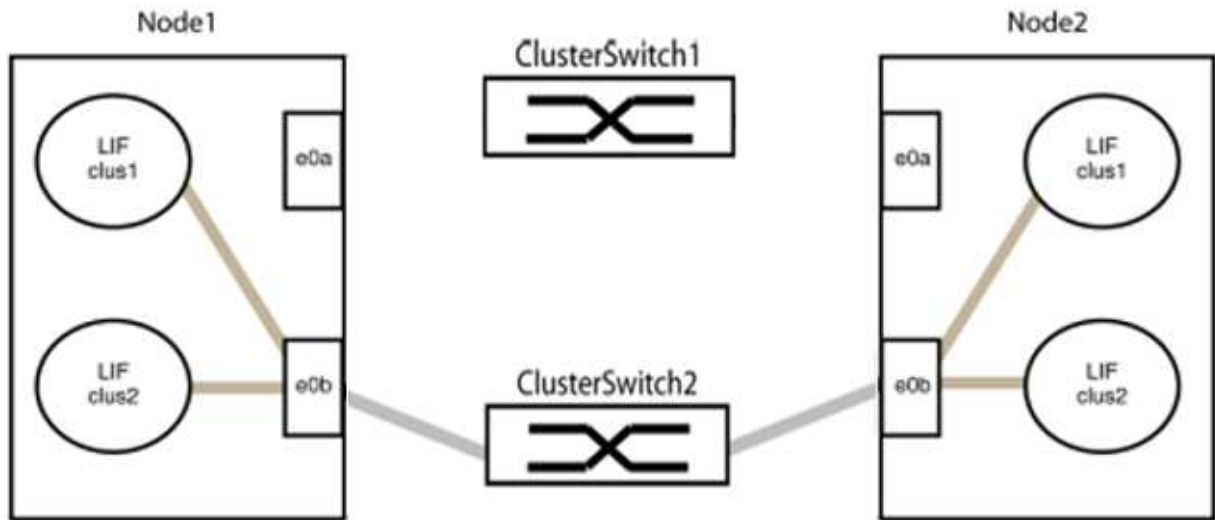
2. Impostare la configurazione senza switch per le porte del gruppo 1.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 1 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

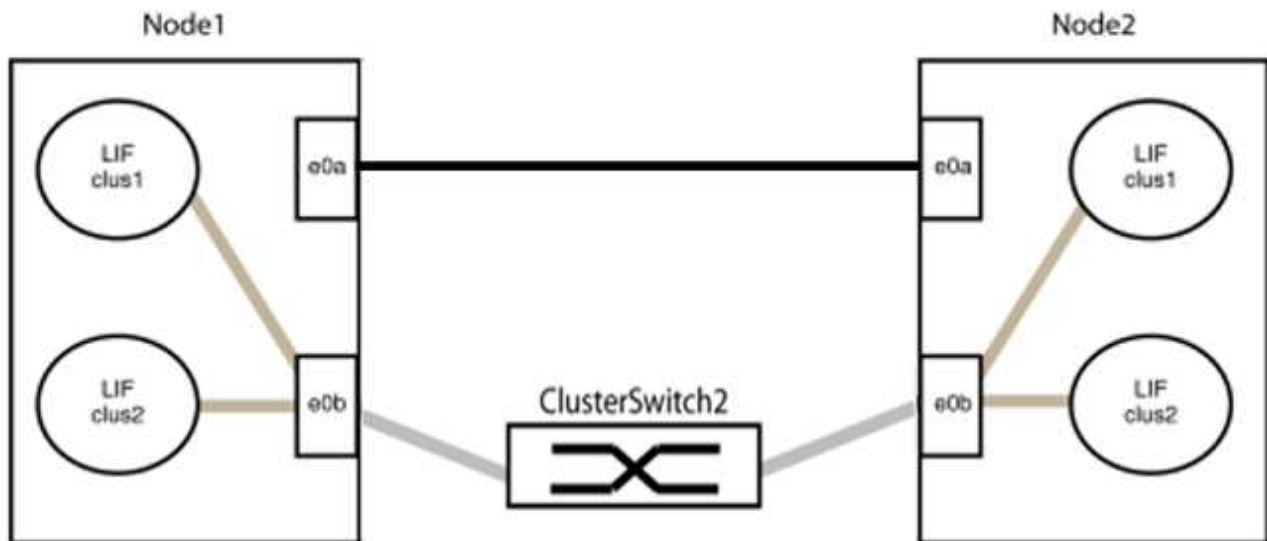
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 1.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0a" su ciascun nodo e il traffico del cluster continua attraverso lo switch e la porta "e0b" su ciascun nodo:



b. Collegare le porte del gruppo 1 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2:



3. L'opzione di rete cluster senza switch passa da `false` A `true` . L'operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione senza interruttore sia impostata su `true` :

```
network options switchless-cluster show
```

L'esempio seguente mostra che il cluster switchless è abilitato:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. 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	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)

```



Prima di procedere al passaggio successivo, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

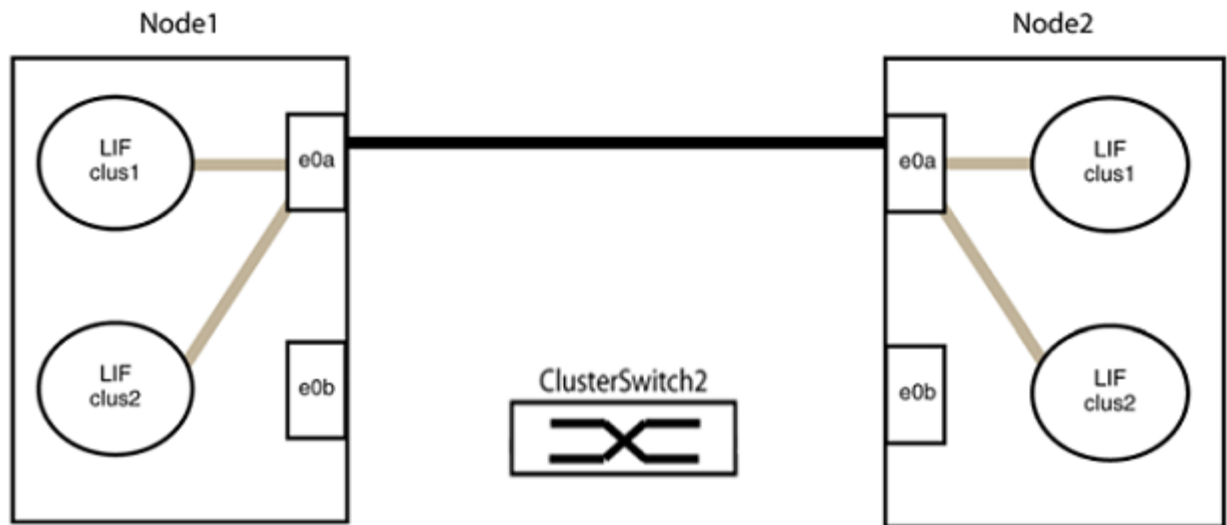
1. Impostare la configurazione senza switch per le porte nel gruppo 2.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

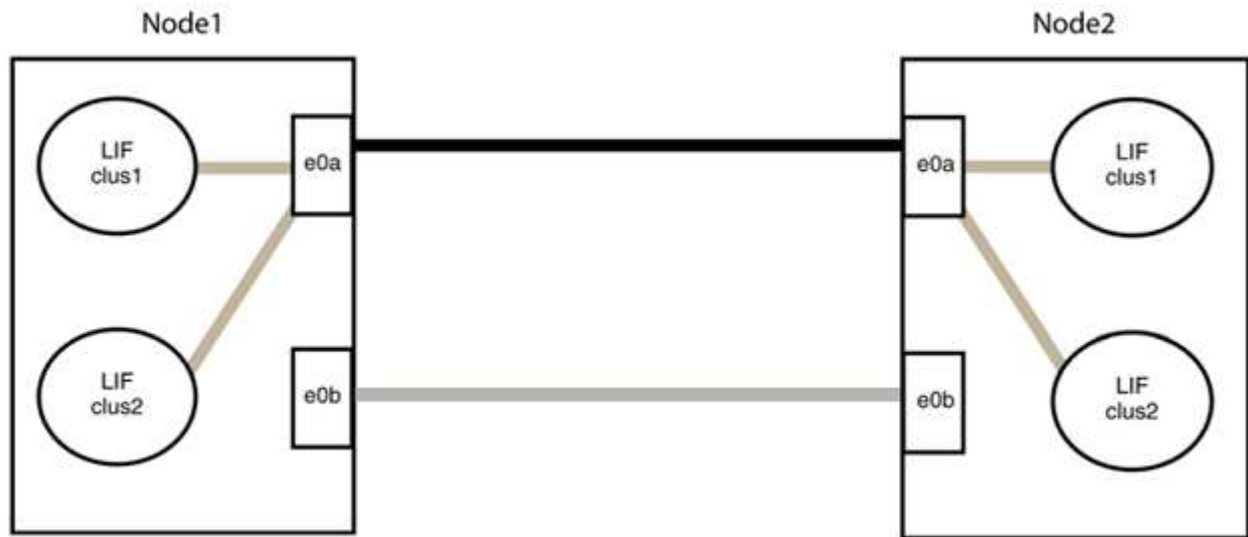
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 2.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua tramite la connessione diretta tra le porte "e0a":



b. Cablare le porte del gruppo 2 una dietro l'altra.

Nell'esempio seguente, "e0a" sul nodo 1 è connesso a "e0a" sul nodo 2 e "e0b" sul nodo 1 è connesso a "e0b" sul nodo 2:



Passaggio 3: verificare la configurazione

1. Verificare che le porte su entrambi i nodi siano collegate correttamente:

```
network device-discovery show -port cluster_port
```

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono correttamente collegate alla porta corrispondente sul partner del cluster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e0a    node2                      e0a        AFF-A300
          e0b    node2                      e0b        AFF-A300
node1/lldp
          e0a    node2 (00:a0:98:da:16:44) e0a        -
          e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
          e0a    node1                      e0a        AFF-A300
          e0b    node1                      e0b        AFF-A300
node2/lldp
          e0a    node1 (00:a0:98:da:87:49) e0a        -
          e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Riattivare il ripristino automatico per i LIF del cluster:

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

3. Verificare che tutti i LIF siano a casa. Potrebbero volerci alcuni secondi.

```
network interface show -vserver Cluster -lif lif_name
```

Mostra esempio

I LIF sono stati ripristinati se la colonna "È a casa" è true , come mostrato per node1_clus2 E node2_clus2 nell'esempio seguente:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Se uno qualsiasi dei LIFS del cluster non è tornato alle proprie porte home, ripristinarlo manualmente dal nodo locale:

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

4. Controllare lo stato del cluster dei nodi dalla console di sistema di uno dei due nodi:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra epsilon su entrambi i nodi da false :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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. Se hai disattivato la creazione automatica dei casi, riattivala richiamando un messaggio AutoSupport :

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

Per maggiori informazioni, vedere ["Articolo 1010449 della Knowledge Base NetApp : Come sopprimere la creazione automatica di casi durante le finestre di manutenzione programmata"](#).

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

Cosa succederà ora?

Dopo aver sostituito gli interruttori, puoi ["configurare il monitoraggio dello stato dello switch"](#).

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.