Switch del cluster

Install and maintain

NetApp
November 07, 2025

This PDF was generated from https://docs.netapp.com/it-it/ontap-systems-switches/switch-bes-53248/configure-new-switch-overview.html on November 07, 2025. Always check docs.netapp.com for the latest.

Sommario

Switch del cluster . . . 1
- BES-53248 supportato da Broadcom . . . 1
  - Inizia subito . . . 1
  - Installare l’hardware . . . 5
  - Configurare il software . . . 8
  - Aggiorna lo switch . . . 106
  - Migrare gli switch . . . 150
  - Sostituire gli interruttori . . . 186
- Cisco Nexus 9336C-FX2 o 9336C-FX2-T. . . . 214
  - Inizia subito . . . 214
  - Installare l’hardware . . . 220
  - Configurare il software . . . 231
  - Migrare gli switch . . . 302
  - Sostituire gli interruttori . . . 354
- NVIDIA SN2100 . . . 386
  - Inizia subito . . . 386
  - Installare l’hardware . . . 389
  - Configurare il software . . . 398
  - Migrare gli switch . . . 475
  - Sostituire gli interruttori . . . 530

Switch del cluster

BES-53248 supportato da Broadcom

Inizia subito

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, consultare i requisiti di configurazione e supporto EFOS e ONTAP.

Supporto EFOS e ONTAP

Vedere "NetApp Hardware Universe" e. "Matrice di compatibilità degli switch Broadcom" Per informazioni sulla compatibilità EFOS e ONTAP con gli switch BES-53248. Il supporto di EFOS e ONTAP può variare in base al tipo di macchina specifico dello switch BES-53248. Per informazioni dettagliate su tutti i tipi di switch BES-52348, vedere "Componenti e codici ricambio per switch cluster BES-53248".

Requisiti di configurazione

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

Assegnazioni delle porte dello switch del cluster

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

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

Vedere "Hardware Universe" per ulteriori informazioni sulle porte dello switch.

Limite di velocità del gruppo di porte

- Sugli switch cluster BES-53248, le porte 48 10/25GbE (SFP28/SFP+) sono combinate in 12 gruppi a 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 si acquistano licenze aggiuntive, vedere "Attivare le nuove porte delle licenze" per ulteriori informazioni su come attivarle.
- 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 codici ricambio per switch cluster BES-53248

Per l'installazione e la manutenzione dello switch BES-53248, consultare l'elenco dei componenti e dei codici.

La seguente tabella elenca il numero di parte, la descrizione e le versioni minime di EFOS e ONTAP per i componenti dello switch cluster BES-53248, inclusi i dettagli del kit per montaggio su rack.

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

Codice del ricambio	Descrizione	Versione minima di EFOS	Versione minima di ONTAP
X190005-B.	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = scarico laterale porta)	3.10.0.3	9.8
X190005R-B.	BES-53248-B/IX8, CLSW, 16PT10/25GB, PSIN (PSIN = Port Side Intake)	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 guide per montaggio in rack Ozeki a 4 montanti da 19"	N/A.	N/A.

Prendere nota delle seguenti informazioni relative ai tipi di macchina:

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

È possibile determinare il tipo di macchina specifico 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................................... QTWCU225xxxxx
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 della documentazione per gli switch cluster BES-53248

Per l'installazione e la manutenzione dello switch BES-53248, consultare la documentazione relativa a switch e controller specifici.

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
EFOS Administrator's Guide v3.4.3	Vengono forniti esempi di come utilizzare lo switch BES-53248 in una rete tipica.
EFOS CLI Command Reference v3.4.3	Descrive i comandi dell'interfaccia a riga di comando (CLI) utilizzati per visualizzare e configurare il software BES-53248.
EFOS Getting Started Guide v3.4.3	Fornisce informazioni dettagliate su per lo switch BES-53248.

Titolo del documento	Descrizione
EFOS SNMP Reference Guide v3.4.3	Vengono forniti esempi di come utilizzare lo switch BES-53248 in una rete tipica.
Parametri e valori di scalabilità EFOS v3.4.3	Descrive i parametri di scalabilità predefiniti con cui il software EFOS viene fornito e validato sulle piattaforme supportate.
Specifiche funzionali EFOS v3.4.3	Descrive le specifiche del software EFOS sulle piattaforme supportate.
EFOS Release Notes v3.4.3	Fornisce informazioni specifiche sulla versione del software BES-53248.
Matrice di compatibilità di rete per la gestione e la rete del cluster	Fornisce informazioni sulla compatibilità di rete. La matrice è disponibile sul sito di download dello switch BES-53248 all'indirizzo "Switch di cluster Broadcom".

Documentazione sui sistemi ONTAP e articoli della Knowledge base

Per configurare un sistema ONTAP, è necessario disporre dei seguenti documenti dal sito del supporto NetApp all'indirizzo "mysupport.netapp.com" Oppure il sito della Knowledge base (KB) all'indirizzo "kb.netapp.com".

Nome	Descrizione
"NetApp Hardware Universe"	Descrive i requisiti di alimentazione e di sito per tutto l'hardware NetApp, inclusi gli armadi di sistema, e fornisce informazioni sui connettori e sulle opzioni dei cavi da utilizzare insieme ai relativi codici ricambio.
Istruzioni di installazione e configurazione specifiche del controller	Descrive come installare l'hardware NetApp.
ONTAP 9	Fornisce informazioni dettagliate su tutti gli aspetti di ONTAP 9.
Aggiunta di licenze aggiuntive per le porte per lo switch BES-53248 supportato da Broadcom	Fornisce informazioni dettagliate sull'aggiunta di licenze per le porte. Accedere alla "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:

1. **"Installare l'hardware dello switch"**

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

2 "Analisi del cablaggio e della 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, consultare la documentazione di Broadcom.

Fasi

1. Esaminare "requisiti di configurazione".
2. Seguire le istruzioni in "Guida all'installazione dello switch cluster BES-53248 supportato da Broadcom".

Quali sono le prossime novità?

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

Esaminare le considerazioni relative al cablaggio e alla configurazione

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

Assegnazione degli switch delle porte del cluster

È possibile utilizzare la tabella di assegnazione delle porte degli switch cluster BES-53248 supportata da Broadcom come guida alla configurazione del cluster.

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

Vedere "Hardware Universe" per ulteriori informazioni sulle porte dello switch.

Limite di velocità del gruppo di porte

- Sugli switch cluster BES-53248, le porte 48 10/25GbE (SFP28/SFP+) sono combinate in 12 gruppi a 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 le porte 25g con cavi in rame, vedere la tabella seguente per i dettagli.

  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 tabella seguente 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 Bootarg

Utilizzare il seguente comando per impostare il FEC della porta 25g su uno dei due `auto` oppure `fc`, secondo necessità:

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

- Quando è impostato su **`auto`**:
  - Il `auto` l'impostazione propaga immediatamente l'impostazione all'hardware e non è necessario riavviare il sistema.
  - Se `bootarg.cpk_fec_fc_eXx already exists`, viene eliminato dall'archivio di avvio.
  - Dopo un riavvio, l' `auto` l'impostazione rimane attiva da allora `auto` È l'impostazione FEC predefinita.
- Quando è impostato su **`fc`**:
  - Il `FC-FEC` l'impostazione propaga immediatamente l'impostazione all'hardware e non è necessario riavviare il sistema.
  - Un nuovo `bootarg.cpk_fec_fc_eXx` viene creato con il valore impostato su "true".
  - Dopo un riavvio, `FC-FEC` l'impostazione rimane attiva per l'utilizzo del codice conducente.

Configurare il software

Workflow di installazione del software per switch BES-53248

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

1. **"Configurare lo switch"**

Configurare lo switch cluster BES-53248.

2. **"Installare il software EFOS"**

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

3. **"Installare le licenze per gli switch cluster BES-53248"**

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

4. **"Installazione del file di configurazione di riferimento (RCF)"**

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

5. **"Abilitare SSH sugli switch cluster BES-53248"**

Se si utilizzano le funzioni CSHM (Ethernet Switch Health Monitor) e di raccolta dei registri, attivare SSH sugli switch.

6 **"Ripristinare l'interruttore alle impostazioni predefinite di fabbrica"**

Cancellare le impostazioni dello switch del cluster BES-53248.

Configurare lo switch del cluster BES-53248

Seguire questa procedura per eseguire una configurazione iniziale dello switch del cluster BES-53248.

Prima di iniziare

- Viene installato l'hardware, come descritto in "Installare l'hardware".
- Hai esaminato quanto segue:
  - "Requisiti di configurazione"
  - "Componenti e numeri di parte"
  - "Requisiti di documentazione"

A proposito degli esempi

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

- I nomi degli switch NetApp sono `cs1` e. `cs2`. L'aggiornamento inizia dal secondo switch, *cs2.*
- I nomi LIF del cluster sono `node1_clus1` e. `node1_clus2` per il node1, e. `node2_clus1` e. `node2_clus2` per il node2.
- Il nome IPSpace è Cluster.
- Il `cluster1::>` prompt indica il nome del cluster.
- Le porte del cluster su ciascun nodo sono denominate `e0a` e. `e0b`. Vedere "NetApp Hardware Universe" per le porte cluster effettivamente supportate sulla 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.
- Gli esempi utilizzano due nodi, ma è possibile includere fino a 24 nodi in un cluster.

Fasi

1. Collegare la porta seriale a una porta host o 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. Accedere allo switch come `admin` E premere **Invio** quando viene richiesta una password. Il nome predefinito dello switch è **routing**. Quando richiesto, immettere `enable`. In questo modo è possibile

accedere alla modalità EXEC privilegiata per la configurazione dello switch.

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

5. Modificare 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

serviceport è impostato su Usa DHCP per impostazione predefinita. L'indirizzo IP, la subnet mask 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

serviceport è impostato su Usa DHCP per impostazione predefinita. L'indirizzo IP, la subnet mask 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 server dei nomi:

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

EFOS 3.10.0.3 e versioni successive

Configurare manualmente l'ora.

`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 versioni precedenti

Configurare manualmente l'ora.

`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!
```

Quali sono le prossime novità?

Dopo aver configurato gli switch, puoi "installare il software EFOS".

Installare il software EFOS

Per installare il software Ethernet Fabric OS (EFOS) sullo switch cluster BES-53248, procedere come segue.

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

Preparazione per l'installazione

Prima di iniziare

- Questa procedura è adatta solo per installazioni nuove.
- Scaricare il software Broadcom EFOS applicabile per gli switch del cluster da "Supporto per switch Ethernet Broadcom" sito.
- Assicurarsi che "Lo switch del cluster BES-53248 è configurato".

Installare il software

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

- Metodo 1: Installare EFOS. Utilizzare per la 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 è conforme a FIPS.

Metodo 1: Installare EFOS

Per installare il software EFOS, procedere come segue.

Fasi

1. Accedere alla porta seriale della console dello switch o connettersi con SSH.
2. Utilizzare `ping` 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. Scaricare il file immagine sullo switch.

   Consultare la tabella seguente per informazioni sui protocolli di copia supportati:

Protocollo	Prerequisito
TFTP (Trivial file Transfer Protocol)	Nessuno
SFTP (SSH file Transfer Protocol)	Il pacchetto software deve supportare una gestione sicura
FTP	Password obbligatoria
XMODEM	Nessuno
YMODEM	Nessuno
ZMODEM	Nessuno
Protocollo SCP (Secure Copy Protocol)	Il pacchetto software deve supportare una 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

   Copiare il file immagine nell'immagine attiva significa che quando si riavvia, l'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. Visualizzare 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. Effettuare nuovamente l'accesso e verificare 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 l'interruttore, procedere come segue:
   a. "Installare le licenze"
   b. "Installare il file RCF"
   c. "Abilitare SSH"
   d. "Abilitare la raccolta dei log"
   e. "Configurare SNMPv3 per il monitoraggio"
8. Ripetere i passaggi da 1 a 7 sullo switch partner.

Metodo 2: Installare EFOS in modalità ONIE

Se una versione di EFOS è conforme a FIPS e l'altra non è conforme a FIPS, eseguire le seguenti operazioni. Questa procedura può essere utilizzata per installare l'immagine EFOS 3.7.x.x non conforme a FIPS o FIPS da ONIE in caso di mancato avvio dello switch.

Fasi

1. Collegare 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

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

Dopo aver selezionato **ONIE**, lo switch si carica e presenta diverse opzioni. 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 il rilevamento 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:/ #
```

   Il rilevamento 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 routing 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. Installare 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 riavvia lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione di EFOS.

7. Accedere e 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 viene riavviato senza alcuna configurazione applicata e viene ripristinato i valori predefiniti. Per riconfigurare l'interruttore, procedere come segue:
   a. "Configurare lo switch"
   b. "Installare le licenze"
   c. "Installare il file RCF"
   d. "Abilitare SSH"

e. "Abilitare la raccolta dei log"

f. "Configurare SNMPv3 per il monitoraggio"

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 del cluster BES-53248.

> Tutte le porte vengono configurate durante l'installazione di RCF, ma è necessario installare la licenza per attivare le porte configurate.

Verifica dei requisiti

Prima di iniziare

Verificare che siano stati installati i seguenti componenti:

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- RCF corrente, disponibile nella "Broadcom Cluster Switch" pagina.
- Una configurazione di boot in RCF che rifletta le immagini di boot desiderate, necessaria se si installa solo EFOS e si mantiene la versione corrente di RCF. Se è necessario modificare la configurazione di avvio per riflettere le immagini di avvio correnti, è necessario farlo prima di riapplicare RCF in modo che venga creata un'istanza della versione corretta in caso di riavvio futuro.
- Una connessione console allo switch, necessaria quando si installa RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se si è 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 consigliata

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedere "Download del software EFOS" pagina. Si noti che esistono dipendenze di comando tra la sintassi del comando in RCF e quella presente nelle versioni di EFOS.

Installare il file di configurazione

A proposito degli esempi

Gli esempi di 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::*>` prompt indica il nome del cluster.
- Gli esempi di questa procedura utilizzano quattro nodi. Questi nodi utilizzano due porte di interconnessione

cluster da 10 GbE `e0a` e. `e0b`. Vedere "Hardware Universe" per verificare le porte cluster corrette sulle piattaforme.

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

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Broadcom switch; i comandi ONTAP vengono utilizzati se non diversamente indicato.

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

Prima di installare una nuova versione del software dello switch e RCF, consultare 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, eseguire nuovamente la configurazione di base. È necessario essere collegati allo switch utilizzando la console seriale perché una cancellazione completa della configurazione ripristina la configurazione della rete di gestione.

Fase 1: Preparazione per l'installazione

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

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

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

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

   Il seguente comando elimina la creazione automatica del caso per due ore:

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

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

```
network device-discovery show
```

Mostra esempio

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       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 ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

Mostra esempio

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

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  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 relative a 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 versioni 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. Disattiva il ripristino automatico sulle LIF del cluster.

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

Fase 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, spegnere le porte collegate alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono connesse 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 le LIF del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   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 funzioni correttamente:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se non è già stato fatto, salvare la configurazione corrente dello switch copiando l'output del seguente comando in un file di log:

```
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 collegati allo switch utilizzando la console seriale. Questo requisito è facoltativo se si è 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 comporta l'eliminazione delle licenze.

a. SSH nello switch.

   Procedere solo quando tutte le LIF del cluster sono state rimosse dalle porte dello switch e lo switch è pronto per cancellare la configurazione.

b. Accedere alla modalità privilegio:

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

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

```
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. Riavviare lo switch:

```
(cs2)# reload

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

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

7. Registrare eventuali personalizzazioni effettuate nell'RCF precedente e applicarle al nuovo RCF. Ad esempio, l'impostazione delle velocità delle porte o la modalità FEC con codifica rigida.
8. Copiare l'RCF nella memoria di avvio dello switch CS2 utilizzando uno dei seguenti protocolli di trasferimento: FTP, HTTP, TFTP, SFTP o SCP.

   In questo esempio viene illustrato l'utilizzo di HTTP per copiare un RCF nel bootflash dello 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. Verificare che lo script sia stato scaricato e salvato con il nome file assegnato:

   `script list`

```
(cs2)# script list

Configuration Script Name                 Size(Bytes)  Date of
Modification
----------------------------------------  -----------
--------------------
Reference-config.scr                      2680         2024 05 31
21:54:22
1 configuration script(s) found.
2045 Kbytes free.
```

10. Applicare 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. 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 aggiuntive con licenza appaiano dopo l'applicazione dell'RCF:

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

Mostra esempio

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

                Admin     Physical     Physical   Link   Link
LACP   Actor
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, verificare 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, visualizzare le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono connesse 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

                                Link    Physical    Physical
Media       Flow
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 funzionanti e funzionanti in tutti i nodi del cluster:

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

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02


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

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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 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 relative a 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 versioni 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. sullo switch del cluster CS1, chiudere le porte collegate alle porte del cluster dei nodi.

   Nell'esempio seguente viene utilizzato 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 le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current  Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port     Home
----------- ------------------ ---------- ------------------
------------------ -------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01        e0a      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 funzioni correttamente:

   `cluster show`

   Mostra esempio

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
```

4. Ripetere i passaggi da 4 a 19 sull'interruttore CS1.

5. Abilitare il ripristino automatico sulle LIF del cluster:

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

6. Riavviare l'interruttore CS1. In questo modo, le LIF del cluster tornano alle porte home. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati 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!
```

Fase 3: Verificare la configurazione

1. Sullo switch CS1, verificare che le porte dello switch collegate alle porte del cluster siano **up**:

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

Mostra esempio

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

                                Link    Physical    Physical
Media       Flow
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 funzioni correttamente:

```
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 le LIF del cluster siano tornate alla porta home:

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         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 funzioni correttamente:

   `cluster show`

Mostra esempio

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. Modificare nuovamente il livello di privilegio in admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver installato il file RCF e la licenza, puoi "abilita SSH".

Installare le licenze per gli switch cluster BES-53248

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

Per EFOS 3,12 e versioni successive, seguire la procedura di installazione descritta in "Installare il file di configurazione di riferimento (RCF) e il file di licenza".

Esaminare le licenze disponibili

Sullo switch cluster BES-53248 sono disponibili le seguenti licenze:

Tipo di licenza	Dettagli della licenza	Versione del firmware supportata
SW-BES-53248A2-8P-2P	Broadcom 8PT-10G25G + chiave di licenza 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 a 6 porte 40G100G, X190005/R.	EFOS 3.4.4.6 e versioni successive

Licenze legacy

La seguente tabella elenca le licenze legacy disponibili per l'utilizzo sullo switch cluster BES-53248:

Tipo di licenza	Dettagli della licenza	Versione del firmware supportata
SW-BES-53248A1-G1-8P-LIC	Broadcom 8P 10-25,2P40-100, chiave di licenza, X190005/R.	EFOS 3.4.3.3 e versioni successive
SW-BES-53248A1-G1-16P-LIC	Broadcom 16P 10-25,4P40-100, chiave di licenza, X190005/R.	EFOS 3.4.3.3 e versioni successive

Tipo di licenza	Dettagli della licenza	Versione del firmware supportata
SW-BES-53248A1-G1-24P-LIC	Broadcom 24P 10-25,6P40-100, chiave di licenza, 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 16 Port 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

Non è richiesta una licenza per la configurazione di base.

Installare i file di licenza

Per installare le licenze per gli switch cluster BES-53248, procedere come segue.

Fasi

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare `ping` 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. Verificare l'utilizzo corrente della licenza sullo 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 più licenze e utilizzare numeri di indice delle chiavi diversi.

   Mostra esempio

   Nell'esempio seguente viene utilizzato SFTP per copiare un file di licenza in un indice delle chiavi 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. Visualizzare tutte le informazioni sulla licenza corrente e annotare lo stato della licenza prima del riavvio dello 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 concesse in licenza:

   `show port all | exclude Detach`

   Le porte dei file di licenza aggiuntivi non vengono visualizzate fino a quando lo switch non viene riavviato.

Mostra esempio

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

                Admin     Physical   Physical   Link   Link    LACP
Actor
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

                Admin     Physical   Physical   Link   Link    LACP
Actor
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 uno switch di produzione funzionante.

Risolvere i problemi di installazione

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

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 si esegue `copy` con il `debug transfer` e. `debug license` opzioni attivate, viene restituito l'output del log.

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.
```

Verificare quanto segue nell'output di debug:

- Verificare che il numero di serie corrisponda a: `Serial number QTFCU38290012 matched.`
- Verificare che il modello dello switch corrisponda a: `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 visualizzato il seguente errore: `License file /mnt/download//license.dat.1 already exists.`
- Una licenza porta non è una licenza funzione. Pertanto, è prevista la seguente dichiarazione: `Feature not found in license file with index = 1.`

Utilizzare `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 eseguire il downgrade del software dello switch dalla versione 3.4.4.6, le licenze vengono rimosse. Questo è il comportamento previsto.

È necessario installare una licenza precedente appropriata prima di tornare a una versione precedente del software.

Attivare le nuove porte con licenza

Per attivare le nuove porte con licenza, è necessario modificare l'ultima versione di RCF e rimuovere i commenti relativi ai dettagli della porta.

La licenza predefinita attiva le porte da 0/1 a 0/16 e da 0/55 a 0/56, mentre le nuove porte con licenza si trovano 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 i commenti dalla seguente sezione dell'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, rimuovere il commento da ciascuna porta, ma rimuovere solo una linea **speed** nell'RCF per ciascuna di queste porte: **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, rimuovere i commenti dall'intera sezione a 8 porte quando è stata attivata una licenza appropriata.

Quali sono le prossime novità?

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

Installazione del file di configurazione di riferimento (RCF)

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

Per EFOS 3,12 e versioni successive, seguire la procedura di installazione descritta in "Installare il file di configurazione di riferimento (RCF) e il file di licenza".

Verifica dei requisiti

Prima di iniziare

Verificare che siano stati installati i seguenti componenti:

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Il file RCF corrente, disponibile da "Broadcom Cluster Switch" pagina.
- Una configurazione di boot in RCF che rifletta le immagini di boot desiderate, necessaria se si installa solo EFOS e si mantiene la versione corrente di RCF. Se è necessario modificare la configurazione di avvio per riflettere le immagini di avvio correnti, è necessario farlo prima di riapplicare RCF in modo che venga creata un'istanza della versione corretta in caso di riavvio futuro.
- Una connessione console allo switch, necessaria quando si installa RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se si è 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 consigliata

Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedere "Download del software EFOS" pagina. Si noti che esistono dipendenze di comando tra la sintassi del comando in RCF e quella presente nelle versioni di EFOS.

Installare il file di configurazione

A proposito degli esempi

Gli esempi di 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::*>` prompt indica il nome del cluster.
- Gli esempi di questa procedura utilizzano quattro nodi. Questi nodi utilizzano due porte di interconnessione cluster da 10 GbE `e0a` e. `e0b`. Vedere "Hardware Universe" per verificare le porte cluster corrette sulle piattaforme.

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

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Broadcom switch; i comandi ONTAP vengono utilizzati se non diversamente indicato.

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

Prima di installare una nuova versione del software dello switch e RCF, consultare 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, eseguire nuovamente la configurazione di base. È necessario essere collegati allo switch utilizzando la console seriale perché una cancellazione completa della configurazione ripristina la configurazione della rete di gestione.

Fase 1: Preparazione per l'installazione

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

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

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

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

   Il seguente comando elimina la creazione automatica del caso per due ore:

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

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

```
set -privilege advanced
```

Viene visualizzato il prompt Advanced (*>).

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

```
network device-discovery show
```

Mostra esempio

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       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 ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

Mostra esempio

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

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  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 relative a 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 versioni 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. Disattiva il ripristino automatico sulle LIF del cluster.

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

Fase 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, spegnere le porte collegate alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono connesse 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 le LIF del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   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 funzioni correttamente:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se non è già stato fatto, salvare la configurazione corrente dello switch copiando l'output del seguente comando in un file di log:

```
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 collegati allo switch utilizzando la console seriale. Questo requisito è facoltativo se si è 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 comporta l'eliminazione delle licenze.

a. SSH nello switch.

   Procedere solo quando tutte le LIF del cluster sono state rimosse dalle porte dello switch e lo switch è pronto per cancellare la configurazione.

b. Accedere alla modalità privilegio:

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

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

```
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. Riavviare lo switch:

```
(cs2)# reload

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

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

7. Tenere presente quanto segue:

a. Se sullo switch sono state installate licenze porta aggiuntive, è necessario modificare l'RCF per configurare le porte aggiuntive con licenza. Vedere "Attivare le nuove porte con licenza" per ulteriori informazioni.

b. Registrare eventuali personalizzazioni effettuate nell'RCF precedente e applicarle al nuovo RCF. Ad esempio, l'impostazione delle velocità delle porte o la modalità FEC con codifica rigida.

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 l'utilizzo di SFTP per copiare un RCF nella flash di avvio 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. Verificare che lo script sia stato scaricato e salvato con il nome file 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. Applicare 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 di 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 l'utilizzo di SFTP per copiare un RCF nella flash di avvio 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. Verificare che lo script sia stato scaricato e salvato con il nome file assegnato:

   ```
   script list
   ```

```
(cs2)# script list

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

1 configuration script(s) found.
```

2. Applicare 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. 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 aggiuntive con licenza appaiano dopo l'applicazione dell'RCF:

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

Mostra esempio

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

                Admin     Physical     Physical   Link   Link
LACP   Actor
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
```

```
(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, visualizzare le porte connesse alle porte del cluster dei nodi. Ad esempio, se le porte da 0/1 a 0/16 sono connesse 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

                                Link    Physical    Physical
Media       Flow
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 funzionanti e funzionanti in tutti i nodi del cluster:

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

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02


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

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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 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 relative a 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 versioni 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. sullo switch del cluster CS1, chiudere le porte collegate alle porte del cluster dei nodi.

   Nell'esempio seguente viene utilizzato 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 le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current  Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port     Home
----------- ------------------ ---------- ------------------
------------------ -------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01        e0a      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 funzioni correttamente:

   `cluster show`

   Mostra esempio

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
```

4. Ripetere i passaggi da 4 a 19 sull'interruttore CS1.

5. Abilitare il ripristino automatico sulle LIF del cluster:

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

6. Riavviare l'interruttore CS1. In questo modo, le LIF del cluster tornano alle porte home. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati 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!
```

Fase 3: Verificare la configurazione

1. Sullo switch CS1, verificare che le porte dello switch collegate alle porte del cluster siano **up**:

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

Mostra esempio

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

                                Link    Physical    Physical
Media       Flow
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 funzioni correttamente:

```
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 le LIF del cluster siano tornate alla porta home:

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         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 funzioni correttamente:

   `cluster show`

Mostra esempio

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. Modificare nuovamente il livello di privilegio in admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver installato l'RCF, puoi "abilita SSH".

Abilitare SSH sugli switch cluster BES-53248

Se si utilizzano le funzioni Ethernet Switch Health Monitor (CSHM) e di raccolta dei log, è necessario generare le chiavi SSH e quindi abilitare SSH sugli switch del cluster.

Fasi

1. Verificare che SSH sia disattivato:

   ```
   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 **FIPS-mode**):

   In modalità FIPS, le chiavi devono essere crittografate con una passphrase per la protezione. In assenza di una chiave crittografata, l'applicazione non si avvia. Le chiavi vengono create e crittografate utilizzando i seguenti comandi:

Mostra esempio

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

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
<passphase>

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
<passphase>

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 attivato:

```
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
```

Quali sono le prossime novità?

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.

A proposito di questa attività

- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

Fasi

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 prompt simile al seguente:

```
(Routing)>
```

Aggiorna lo switch

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

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

1. **"Aggiornare la versione EFOS"**

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

2. **"Aggiornare la versione RCF"**

Aggiornare l'RCF sullo switch del cluster BES-53248, quindi verificare la presenza di una licenza aggiuntiva nelle porte dopo l'applicazione dell'RCF.

3. **"Verificare la rete del cluster ONTAP dopo l'aggiornamento"**

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

Aggiornare il software EFOS

Per aggiornare il software EFOS sullo switch del cluster BES-53248, procedere come

segue.

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

Preparatevi per l'aggiornamento

Prima di iniziare

- Scaricare il software Broadcom EFOS applicabile per gli switch del cluster da "Supporto per switch Ethernet Broadcom" sito.
- Leggere le seguenti note relative alle versioni di EFOS.

Nota:

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

Procedura	Versione EFOS corrente	Nuova versione EFOS	Fasi di alto livello
Procedura per l'aggiornamento di EFOS tra due versioni (non) conformi a FIPS	3.4.x.x	3.4.x.x	Aggiornare la nuova immagine EFOS utilizzando Metodo 1: Aggiornamento EFOS. Le informazioni di configurazione e licenza vengono conservate.

3.4.4.6 (o versione successiva 3.4.x.x)	3.7.x.x o versioni successive non conformi a FIPS	Aggiorna EFOS utilizzando Metodo 1: Aggiornamento EFOS. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.7.x.x o versioni successive.	3.7.x.x o versioni successive non conformi a FIPS
3.4.4.6 (o versione successiva 3.4.x.x)	Eseguire il downgrade di EFOS con Metodo 1: Aggiornamento EFOS. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.4.x.x.	3.7.x.x o versioni successive non conformi a FIPS	
Aggiornare la nuova immagine EFOS utilizzando Metodo 1: Aggiornamento EFOS. Le informazioni di configurazione e licenza vengono conservate.	3.7.x.x o successivo conforme a FIPS	3.7.x.x o successivo conforme a FIPS	Aggiornare la nuova immagine EFOS utilizzando Metodo 1: Aggiornamento EFOS. Le informazioni di configurazione e licenza vengono conservate.
Procedura 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 versione di EFOS in uso è conforme a FIPS o non conforme a FIPS, utilizzare `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.
```

Aggiornare il software

Utilizzare uno dei seguenti metodi:

- Metodo 1: Aggiornamento EFOS. Utilizzare per la maggior parte dei casi (vedere la tabella precedente).
- 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 è conforme a FIPS.

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

Metodo 1: Aggiornamento EFOS

Per aggiornare il software EFOS, procedere come segue.

Si noti che dopo l'aggiornamento degli switch del cluster BES-53248 da EFOS 3,3.x.x o 3,4.x.x a EFOS 3.7.0.4 o 3,8.0,2, i collegamenti interswitch (ISL) e i canali delle porte sono contrassegnati nello stato **down**. Questo è il comportamento previsto ed è sicuro continuare con l'aggiornamento a meno che non si verifichino problemi con la riattivazione automatica delle LIF. Per ulteriori informazioni, consultare l'articolo della Knowledge base: "BES-53248 Cluster Switch NDU non ha eseguito l'aggiornamento a EFOS 3.7.0.4 e versioni successive"

Fasi

1. Collegare lo switch del cluster BES-53248 alla rete di gestione.
2. Utilizzare `ping` 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. Disattiva l'autorevert sulle LIF del cluster.

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

4. Visualizzare 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. Scaricare 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. Visualizzare 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
```

7. Avviare il sistema dalla configurazione di backup:

   `boot system backup`

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

8. Visualizzare 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. Effettuare nuovamente l'accesso e verificare 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 passi da 5 a 11 sull'interruttore CS1.
13. Abilitare il ripristino automatico sulle LIF del cluster.

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

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

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

Per ulteriori dettagli, vedere "Ripristinare la porta home di un LIF".

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

Se una versione di EFOS è conforme a FIPS e l'altra non è conforme a FIPS, eseguire le seguenti operazioni. Questi passaggi possono essere utilizzati per aggiornare l'immagine EFOS 3,7.x.x non conforme a FIPS o FIPS da ONIE in caso di mancato avvio dello switch.

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

Se si aggiorna EFOS utilizzando l'installazione ONIE OS, la configurazione viene ripristinata ai valori predefiniti e le licenze vengono eliminate. È necessario impostare lo switch e installare le licenze e un RCF supportato per riportare lo switch al normale funzionamento.

Fasi

1. Disattiva l'autorevert sulle LIF del cluster.

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

2. Avviare lo switch in modalità di installazione ONIE.

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

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

Dopo aver selezionato **ONIE**, lo switch si carica e presenta diverse opzioni. 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 il rilevamento 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:/ #
```

   Il rilevamento 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. Installare 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 riavvia lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione di 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 viene riavviato senza alcuna configurazione applicata e viene ripristinato i valori predefiniti. Completare i seguenti passaggi per riconfigurare l'interruttore:
   a. "Installare le licenze"
   b. "Installare RCF"
   c. "Abilitare SSH"
   d. "Abilitare la raccolta dei log"

e. "Configurare SNMPv3 per il monitoraggio"

9. Ripetere i passi da 2 a 8 sull'interruttore CS1.
10. Abilitare il ripristino automatico sulle LIF del cluster.

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

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

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

Per ulteriori dettagli, vedere "Ripristinare la porta home di un LIF".

Aggiornamento del file di configurazione di riferimento (RCF)

È possibile aggiornare il file di configurazione di riferimento (RCF) dopo l'aggiornamento dello switch cluster EFOS BES-53248 e dopo l'applicazione di eventuali nuove licenze.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Il file RCF corrente, disponibile da "Broadcom Cluster Switch" pagina.
- Una configurazione di boot in RCF che rifletta le immagini di boot desiderate, necessaria se si installa solo EFOS e si mantiene la versione corrente di RCF. Se è necessario modificare la configurazione di avvio per riflettere le immagini di avvio correnti, è necessario farlo prima di riapplicare RCF in modo che venga creata un'istanza della versione corretta in caso di riavvio futuro.
- Una connessione console allo switch, necessaria quando si installa RCF da uno stato predefinito di fabbrica. Questo requisito è facoltativo se si è 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 consigliata

- Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Vedere "Download del software EFOS" pagina. Si noti che esistono dipendenze di comando tra la sintassi del comando in RCF e quella presente nelle versioni di EFOS.
- Consultare le guide all'aggiornamento e al software appropriate disponibili sul "Broadcom" Per la documentazione completa sulle procedure di upgrade e downgrade dello switch BES-53248.

A proposito degli esempi

Gli esempi di 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::*>` prompt indica il nome del cluster.
- Gli esempi di questa procedura utilizzano quattro nodi. Questi nodi utilizzano due porte di interconnessione cluster da 10 GbE `e0a` e. `e0b`. Vedere "Hardware Universe" per verificare le porte cluster corrette sulle piattaforme.

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

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Broadcom switch; i comandi ONTAP vengono utilizzati se non diversamente indicato.

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

Prima di installare una nuova versione del software dello switch e RCF, consultare 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 essere collegati allo switch mediante la console seriale, poiché una cancellazione completa della configurazione ripristina la configurazione della rete di gestione.

Passaggio 1: Preparazione per l'aggiornamento

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

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

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

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

   Il seguente comando elimina la creazione automatica del caso per due ore:

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

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

```
network device-discovery show
```

Mostra esempio

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       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 ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

Mostra esempio

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

Node: cluster1-01

Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  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 relative a 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 versioni 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. Disattiva il ripristino automatico sulle LIF del cluster.

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

Fase 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 connesse 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 le LIF del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   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 funzioni correttamente:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
```

5. Se non è già stato fatto, salvare la configurazione corrente dello switch copiando l'output del seguente comando in un file di log:

```
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 collegati allo switch utilizzando la console seriale. Questo requisito è facoltativo se si è 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 comporta l'eliminazione delle licenze.

a. SSH nello switch.

   Procedere solo quando tutte le LIF del cluster sono state rimosse dalle porte dello switch e lo switch è pronto per cancellare la configurazione.

b. Accedere alla modalità privilegio:

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

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

```
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. Riavviare lo switch:

```
reload
```

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

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

7. Tenere presente quanto segue:

a. Se sullo switch sono state installate licenze porta aggiuntive, è necessario modificare l'RCF per configurare le porte aggiuntive con licenza. Vedere "Attivare le nuove porte con licenza" per ulteriori informazioni.

b. Registrare eventuali personalizzazioni effettuate nell'RCF precedente e applicarle al nuovo RCF. Ad esempio, l'impostazione delle velocità delle porte o la modalità FEC con codifica rigida.

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 l'utilizzo di SFTP per copiare un RCF nella flash di avvio 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. Verificare che lo script sia stato scaricato e salvato con il nome file 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. Applicare 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 di 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 l'utilizzo di SFTP per copiare un RCF nella flash di avvio 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. Verificare che lo script sia stato scaricato e salvato con il nome file assegnato:

   ```
   script list
   ```

```
(cs2)# script list

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

1 configuration script(s) found.
```

2. Applicare 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. esamina l'output del banner dal `show clibanner` comando. Leggere e seguire queste istruzioni per garantire la corretta configurazione e il corretto funzionamento dello switch.

   `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 aggiuntive con licenza appaiano dopo l'applicazione dell'RCF:

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

Mostra esempio

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

                Admin     Physical     Physical   Link   Link
LACP   Actor
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, visualizzare 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

                                Link    Physical    Physical
Media       Flow
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 funzionanti e funzionanti in tutti i nodi del cluster:

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

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02


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

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health  Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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 dello switch dal cluster:

```
network device-discovery show
```

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
```

10. Verificare che il cluster visualizzi le informazioni relative a 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 versioni 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. ripetere i passaggi da 1 a 20 sull'interruttore CS1.
2. Abilitare il ripristino automatico sulle LIF del cluster:

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

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

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

Per ulteriori dettagli, vedere "Ripristinare la porta home di un LIF".

Fase 3: Verificare la configurazione

1. Sullo switch CS1, verificare che le porte dello switch collegate alle porte del cluster siano **up**:

```
show interfaces status all
```

Mostra esempio

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

                                Link    Physical    Physical
Media       Flow
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 funzioni correttamente:

```
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 le LIF del cluster siano tornate alla porta home:

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0a     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         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 funzioni correttamente:

   `cluster show`

Mostra esempio

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
```

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. Modificare nuovamente il livello di privilegio in admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla 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 l'integrità della rete cluster ONTAP dopo un aggiornamento del software EFOS o RCF per gli switch cluster BES-53248.

Fasi

1. Visualizzare le informazioni sulle porte di rete del 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
```

Quali sono le prossime novità?

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

Migrare gli switch

Migrare gli switch del cluster CN1610 agli switch del cluster BES-53248

Per migrare gli switch del cluster CN1610 in un cluster agli switch del cluster BES-53248 supportati da Broadcom, esaminare i requisiti di migrazione e seguire la procedura di

migrazione.

Sono supportati i seguenti switch del cluster:

- CN1610
- BES-53248

Verifica dei requisiti

Verificare che la configurazione soddisfi i seguenti requisiti:

- Alcune delle porte degli switch BES-53248 sono configurate per funzionare a 10GbE.
- La connettività 10GbE GbE dai nodi agli switch cluster BES-53248 è stata pianificata, migrata e documentata.
- Il cluster funziona correttamente (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 utilizzano la versione più recente del software EFOS.
  - I file di configurazione di riferimento (RCF) sono stati applicati agli switch.
  - Qualsiasi personalizzazione del sito, ad esempio DNS, NTP, SMTP, SNMP, E SSH, sono configurati sui nuovi switch.

Connessioni a nodi

Gli switch del cluster supportano le seguenti connessioni di nodo:

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

> È possibile attivare porte aggiuntive acquistando le licenze delle porte.

Porte ISL

Gli switch del cluster utilizzano le seguenti porte ISL (Inter-Switch link):

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

Il "*NetApp Hardware Universe*" Contiene informazioni sulla compatibilità ONTAP, sul firmware EFOS supportato e sul cablaggio degli switch cluster BES-53248.

Cablaggio ISL

Il cablaggio ISL appropriato è il seguente:

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

Migrare gli switch

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

A proposito degli esempi

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

- Gli esempi utilizzano due nodi, ciascuno dei quali implementa due porte di interconnessione cluster da 10 GbE: `e0a` e. `e0b`.
- L'output dei comandi potrebbe variare a seconda delle diverse versioni del software ONTAP.
- Gli switch CN1610 da sostituire sono `CL1` e. `CL2`.
- Gli switch BES-53248 che sostituiscono gli switch CN1610 sono `cs1` e. `cs2`.
- I nodi sono `node1` e. `node2`.
- Lo switch CL2 viene sostituito prima da cs2, quindi da CL1 da cs1.
- Gli switch BES-53248 sono precaricati con le versioni supportate del file di configurazione di riferimento (RCF) e del sistema operativo Ethernet Fabric (EFOS) con cavi ISL collegati alle porte 55 e 56.
- I nomi LIF del cluster sono `node1_clus1` e. `node1_clus2` per il node1, e. `node2_clus1` e. `node2_clus2` per il node2.

A proposito di questa attività

Questa procedura riguarda 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 ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - Scollegare i cavi da tutte le porte del cluster su tutti i nodi collegati a CL2, quindi utilizzare i cavi supportati per ricollegare le porte al nuovo switch del cluster cs2.
- Lo switch CN1610 CL1 è sostituito dallo switch BES-53248 cs1:
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - Scollegare i cavi da tutte le porte del cluster su tutti i nodi collegati a CL1, quindi utilizzare i cavi supportati per ricollegare le porte al nuovo switch del cluster cs1.

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

Fase 1: Preparazione per la migrazione

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

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

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

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

Il seguente comando elimina la creazione automatica del caso per due ore:

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

Fase 2: Configurare le porte e il 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 **up** 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 **up** 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. Visualizzare 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/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
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 di 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
                                                  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
```

b. Verificare che tutte le interfacce del cluster (LIFF) si trovino sulle 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 versioni 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. Disattiva il ripristino automatico sulle LIF del cluster.

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

2. Sullo switch cluster CL2, chiudere le porte collegate alle porte del cluster dei nodi per eseguire il failover delle 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. Verifica che le LIF del cluster abbiano eseguito il failover sulle porte ospitate nello switch del cluster CL1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            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 funzioni correttamente:

   `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. Verificare lo stato delle connessioni di rete trasferite a 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 spostate devono essere `up`.

7. Controllare le informazioni 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               BES-
53248
node1      /cdp
            e0a    CL1                       0/1
CN1610
            e0b    cs2                       0/1               BES-
53248
```

8. Verificare che i collegamenti della porta dello switch siano integri dal punto di vista dello switch CS2:

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

9. Sullo switch cluster CL1, chiudere le porte collegate alle porte del cluster dei nodi per eseguire il failover delle 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)#
```

Tutte le LIF del cluster eseguono il failover allo switch CS2.

10. Verifica che le LIF del cluster abbiano eseguito il failover alle porte ospitate nello switch CS2. Questa operazione potrebbe richiedere alcuni secondi:

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            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 funzioni correttamente:

    `cluster show`

    Mostra esempio

    ```
    cluster1::*> cluster show
    Node       Health  Eligibility   Epsilon
    ---------- ------- ------------- -------
    node1      true    true          false
    node2      true    true          false
    ```

12. Spostare i cavi di connessione del nodo del cluster da CL1 al nuovo switch cs1.
13. Verificare lo stato delle connessioni di rete trasferite a 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 spostate devono essere `up`.

14. Controllare le informazioni 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               BES-
53248
            e0b    cs2                       0/1               BES-
53248
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
```

15. Verificare che i collegamenti della porta dello switch siano integri 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 **up** 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 **up** 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 quadro strumenti, 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 versioni 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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster.

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

2. Verificare che le LIF del cluster siano ripristinate alle porte home (questa operazione potrebbe richiedere un minuto):

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

   Se le LIF del cluster non sono tornate alla porta home, ripristinarle manualmente:

   ```
   network interface revert -vserver Cluster -lif *
   ```

3. Verificare che il cluster funzioni correttamente:

   ```
   cluster show
   ```

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 è stata eliminata la creazione automatica del caso, riattivarla 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
   ```

Quali sono le prossime novità?

Dopo aver migrato gli switch, puoi "configurare il monitoraggio dello stato dello switch".

Migrare a un ambiente cluster NetApp con switch

Se si dispone di un ambiente di cluster *switchless* a due nodi esistente, è possibile eseguire la migrazione a un ambiente di cluster *switched* a due nodi utilizzando gli switch di 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 10GBASE-T RJ45 integrate per le porte di rete del cluster.

Verifica dei requisiti

Esaminare i seguenti requisiti per l'ambiente cluster.

- Tenere presente che la maggior parte dei sistemi richiede due porte cluster-network dedicate su ciascun controller.
- Assicurarsi che lo switch del cluster BES-53248 sia impostato come descritto in "Sostituire i requisiti" prima di avviare il processo di migrazione.
- Per la configurazione senza switch a due nodi, assicurarsi che:
  - La configurazione senza switch a due nodi è configurata e funziona correttamente.
  - I nodi eseguono ONTAP 9.5P8 e versioni successive. Il supporto per le porte cluster da 40/100 GbE inizia con il firmware EFOS versione 3.4.4.6 e successive.
  - Tutte le porte del cluster si trovano nello stato **up**.
  - Tutte le interfacce logiche del cluster (LIFF) si trovano nello stato **up** e nelle porte home.
- Per la configurazione dello switch cluster BES-53248 supportata 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.
  - Gli switch del cluster sono accessibili dalla console.
  - Le connessioni switch nodo-nodo BES-53248 e switch-to-switch utilizzano cavi Twinax o in fibra.

    Il "*NetApp Hardware Universe*" Contiene informazioni sulla compatibilità ONTAP, sul firmware EFOS supportato e sul cablaggio degli switch BES-53248.
- I cavi ISL (Inter-Switch link) 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 più recente del software.
  - Gli switch BES-53248 sono dotati di licenze porta opzionali, se acquistati.
  - I file di configurazione di riferimento (RCF) vengono applicati agli switch.
- Qualsiasi personalizzazione del sito (SMTP, SNMP e SSH) viene configurata sui nuovi switch.

Vincoli di velocità del gruppo di porte

- Le porte 48 10/25GbE (SFP28/SFP+) vengono combinate in 12 gruppi a 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.

Eseguire la migrazione all'ambiente cluster

A proposito degli esempi

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

- I nomi degli switch BES-53248 sono `cs1` e. `cs2`.
- I nomi delle 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::*>` prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono `e0a` e. `e0b`.

  Il "*NetApp Hardware Universe*" contiene le informazioni più recenti sulle porte cluster effettive per le piattaforme in uso.

Fase 1: Preparazione per la migrazione

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

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

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

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

   Il seguente comando elimina la creazione automatica del caso per due ore:

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

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

   `set -privilege advanced`

   Il prompt avanzato (`*>`).

Fase 2: Configurare le porte e il cablaggio

1. Disattivare tutte le porte attive rivolte ai nodi (non le porte ISL) su entrambi i nuovi switch del cluster cs1 **e** cs2.

   > Non è necessario disattivare le porte ISL.

   L'esempio seguente mostra che le porte rivolte al nodo da 1 a 16 sono disattivate 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 attive:

```
show port-channel
```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono installate 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 installate 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. Visualizzare l'elenco dei dispositivi vicini:

```
show isdp neighbors
```

Questo comando fornisce informazioni sui dispositivi collegati al sistema.

Mostra esempio

Nell'esempio riportato di seguito sono elencati 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
```

Nell'esempio riportato di seguito sono elencati 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 installate:

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

Mostra esempio

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

Node: node1

                                                  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: node2

                                                  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
```

5. Verificare che tutte le LIF del cluster siano operative:

   `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. Disattiva l'autorevert sulle LIF del cluster.

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

7. Scollegare il cavo dalla porta del cluster e0a sul nodo 1, quindi collegare e0a alla porta 1 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.

   Il "*NetApp Hardware Universe*" contiene ulteriori informazioni sul cablaggio.

8. Scollegare il cavo dalla porta del cluster e0a sul nodo 2, quindi collegare e0a alla porta 2 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.
9. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs1.

   L'esempio seguente mostra che le porte da 1 a 16 sono attivate 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 installate:

```
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 tutte le LIF del cluster siano operative:

```
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
false
         node1_clus2  up/up      169.254.49.125/16  node1       e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2       e0a
false
         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

    Nell'esempio seguente vengono visualizzate informazioni sullo stato 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 del cluster e0b sul nodo 1, quindi collegare e0b alla porta 1 sullo switch del cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.
14. Scollegare il cavo dalla porta del cluster e0b sul nodo 2, quindi collegare e0b alla porta 2 sullo switch del cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch BES-53248.
15. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs2.

    L'esempio seguente mostra che le porte da 1 a 16 sono attivate 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 installate:

`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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster.

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

2. Verificare che le LIF del cluster siano ripristinate alle porte home (questa operazione potrebbe richiedere un minuto):

   `network interface show -vserver Cluster`

   Se le LIF del cluster non sono tornate alla porta home, ripristinarle manualmente:

   `network interface revert -vserver Cluster -lif *`

3. Verificare che tutte le interfacce siano visualizzate `true` per `Is Home`:

   `network interface show -vserver Cluster`

   Il completamento di questa operazione potrebbe richiedere alcuni 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
```

4. Verificare che entrambi i nodi dispongano di una connessione a ciascuno 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
```

5. Visualizzare le informazioni relative ai dispositivi di rete rilevati nel 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               BES-
53248
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
```

6. Verificare che le impostazioni siano disattivate:

   `network options switchless-cluster show`

   > Il completamento del comando potrebbe richiedere alcuni minuti. Attendere l'annuncio "3 minuti di scadenza".

   Il `false` l'output dell'esempio seguente mostra che le impostazioni di configurazione sono disattivate:

   ```
   cluster1::*> network options switchless-cluster show
   Enable Switchless Cluster: false
   ```

7. Verificare lo stato dei membri del nodo nel cluster:

   `cluster show`

Mostra esempio

L'esempio seguente mostra informazioni sullo stato e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show

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

8. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. Cambia di nuovo il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

   Mostra esempio

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

   Per ulteriori informazioni, consulta: "Articolo della Knowledge base di NetApp: Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificate"

Quali sono le prossime novità?

Dopo aver migrato gli switch, puoi "configurare il monitoraggio dello stato dello switch".

Sostituire gli interruttori

Requisiti per la sostituzione

Prima di sostituire lo switch, assicurarsi che siano soddisfatte le seguenti condizioni nell'ambiente corrente e sullo switch sostitutivo.

Infrastruttura di rete e cluster esistente

Assicurarsi che:

- Il cluster esistente viene verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
- Tutte le porte del cluster sono **up**.
- Tutte le interfacce logiche del cluster (LIFF) sono amministrative e operative **up** e sulle porte home.
- 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.

Switch cluster sostitutivo BES-53248

Assicurarsi che:

- La connettività di rete di gestione sullo switch sostitutivo è funzionale.
- L'accesso della console allo switch sostitutivo è in posizione.
- Le connessioni dei nodi sono porte da 0/1 a 0/16 con licenza predefinita.
- Tutte le porte ISL (Inter-Switch link) sono disattivate 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 descritto in "Configurare lo switch del cluster BES-53248".

Tutte le personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengono copiate nel nuovo switch.

Attivare la registrazione della console

NetApp consiglia vivamente di attivare la registrazione della console sui dispositivi in uso e di eseguire le seguenti operazioni quando si sostituisce lo switch:

- Lasciare attivato AutoSupport durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione del caso per tutta la durata della manutenzione. Consultare questo articolo della Knowledge base "SU92: Come eliminare la creazione automatica dei casi durante le finestre di manutenzione programmata" per ulteriori dettagli.
- Attivare la registrazione della sessione per qualsiasi sessione CLI. Per istruzioni su come attivare 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 ulteriori informazioni

- "Sito di supporto NetApp"
- "NetApp Hardware Universe"

Sostituire uno switch cluster BES-53248 supportato da Broadcom

Seguire questa procedura per sostituire uno switch del cluster BES-53248 supportato da Broadcom difettoso in una rete cluster. Si tratta di una procedura senza interruzioni (NDU).

A proposito degli esempi

Gli esempi di 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 node1, e. `node2_clus1` e. `node2_clus2` per il node2.
- Il prompt per le modifiche a tutti i nodi del cluster è `cluster1::>`

Sulla topologia

Questa procedura si basa sulla seguente topologia di rete del 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/       Local  Discovered
Protocol    Port   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               Intf      Holdtime  Capability Platform
Port ID
----------------------- --------- --------- ----------
--------------- ---------
node1                   0/1       175       H          FAS2750
e0a
node2                   0/2       152       H          FAS2750
e0a
cs2                     0/55      179       R          BES-53248
0/55
cs2                     0/56      179       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       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
```

Fasi

1. Esaminare "Requisiti per la sostituzione".
2. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

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

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

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

3. Installare il file di configurazione di riferimento (RCF) e l'immagine appropriati sullo switch, newcs2, ed eseguire le operazioni necessarie per la preparazione del sito.

   Se necessario, verificare, scaricare e installare le versioni appropriate del software RCF ed EFOS per il nuovo switch. Se il nuovo switch è stato configurato correttamente e non sono necessari aggiornamenti per il software RCF ed EFOS, passare alla fase 2.

   a. È possibile scaricare il software Broadcom EFOS applicabile per gli switch del cluster da "Supporto per switch Ethernet Broadcom" sito. Seguire la procedura riportata nella pagina di download per scaricare il file EFOS per la versione del software ONTAP che si sta installando.

   b. L'RCF appropriato è disponibile sul sito "Broadcom Cluster Switch" pagina. Seguire la procedura indicata nella pagina di download per scaricare l'RCF corretto per la versione del software ONTAP che si sta installando.

4. Sul nuovo switch, accedere come `admin` e chiudere tutte le porte che verranno collegate alle interfacce del cluster di nodi (porte da 1 a 16).

   > Se sono state acquistate licenze aggiuntive per porte aggiuntive, chiudere anche queste porte.

   Se lo switch che si sta sostituendo non è funzionale e viene spento, i LIF sui nodi del cluster dovrebbero essere già in esecuzione il failover sull'altra porta del cluster per ciascun nodo.

   > Non è richiesta alcuna password per l'immissione `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 tutte le LIF del cluster siano disponibili `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. Spegnere 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 dello switch BES-53248 newcs2.
8. Richiamare le porte ISL 0/55 e 0/56 tra gli switch cs1 e newcs2, quindi verificare lo stato di funzionamento del canale della porta.

   Il link state per il port-channel 1/1 deve essere **up** e tutte le porte membro devono essere True sotto l'intestazione Port Active (porta attiva).

Mostra esempio

Questo esempio abilita le porte ISL 0/55 e 0/56 e visualizza lo stato del collegamento per il canale della 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 collegate alle interfacce del cluster di nodi (porte da 1 a 16).

> Se sono state acquistate licenze aggiuntive per porte aggiuntive, chiudere 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 **up**:

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

Mostra esempio

L'output dovrebbe essere simile a quanto segue:

```
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/auto   -
false
```

11. Sullo stesso nodo utilizzato nel passaggio precedente, attendere che il cluster LIF node1_clus2 sul node1 si ripristinino automaticamente.

Mostra esempio

In questo esempio, LIF node1_clus2 su node1 viene invertito correttamente se `Is Home` è `true` e la porta è e0b.

Il seguente comando visualizza le informazioni relative ai LIF su entrambi i nodi. L'avvio del primo nodo ha esito positivo se `Is Home` è `true` per entrambe le interfacce del cluster e mostrano le assegnazioni di porta corrette, in questo esempio `e0a` e. `e0b` al nodo1.

```
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. Visualizzare le informazioni sui nodi di un cluster:

    `cluster show`

    Mostra esempio

    Questo esempio mostra che lo stato 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 in buone condizioni:

    `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 è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver sostituito gli interruttori, puoi "configurare il monitoraggio dello stato dello switch".

Sostituire gli switch del cluster Broadcom BES-53248 con connessioni senza switch

È possibile migrare da un cluster con una rete cluster commutata a uno in cui due nodi

sono collegati direttamente per ONTAP 9.3 e versioni successive.

Verifica dei requisiti

Linee guida

Consultare le seguenti linee guida:

- La migrazione a una configurazione cluster senza switch a due nodi è un'operazione senza interruzioni. La maggior parte dei sistemi dispone di due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per i 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 funzione 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 e utilizza ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

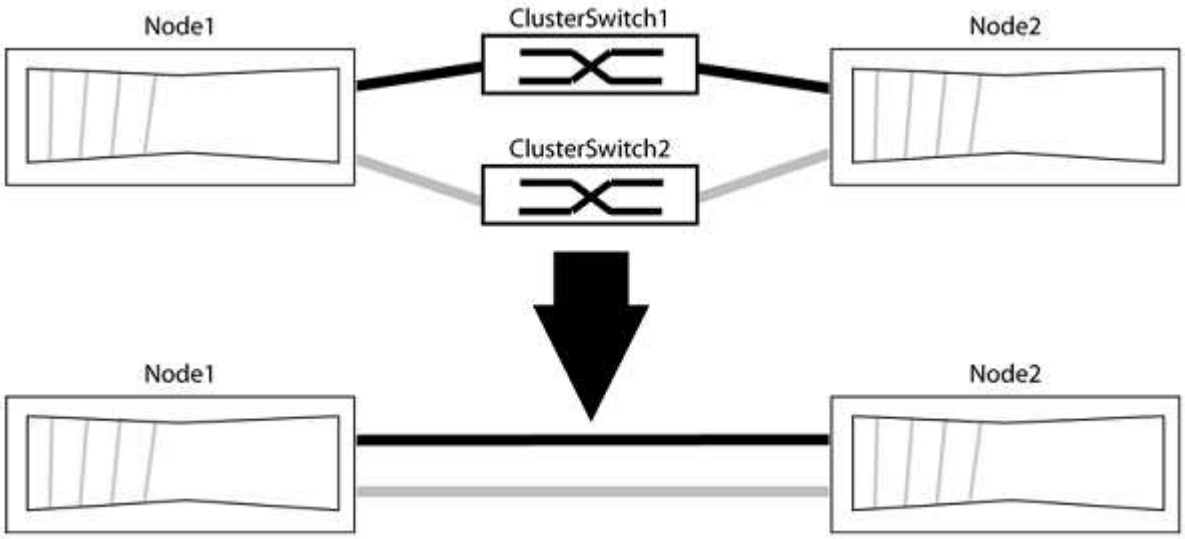
Assicurarsi di disporre di quanto segue:

- Un cluster integro costituito da due nodi collegati da switch di cluster. I nodi devono eseguire la stessa release di ONTAP.
- Ciascun nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, esistono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

A proposito di questa attività

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.



A proposito degli esempi

Gli esempi della seguente procedura mostrano i nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse in base al sistema.

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato `*>` viene visualizzato.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster senza switch, attivato per impostazione predefinita.

   È possibile verificare che il rilevamento dei cluster senza switch sia attivato eseguendo il comando Advanced Privilege:

   ```
   network options detect-switchless-cluster show
   ```

   Mostra esempio

   Il seguente esempio di output mostra se l'opzione è attivata.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Enable Switchless Cluster Detection" (attiva rilevamento cluster senza switch) è `false`, Contattare il supporto NetApp.

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

   ```
   system node autosupport invoke -node * -type all -message
   MAINT=<number_of_hours>h
   ```

   dove `h` indica la durata della finestra di manutenzione in ore. Il messaggio informa il supporto tecnico di questa attività di manutenzione in modo che possa eliminare la creazione automatica del caso durante la finestra di manutenzione.

   Nell'esempio seguente, il comando sospende la creazione automatica del caso per due ore:

   Mostra esempio

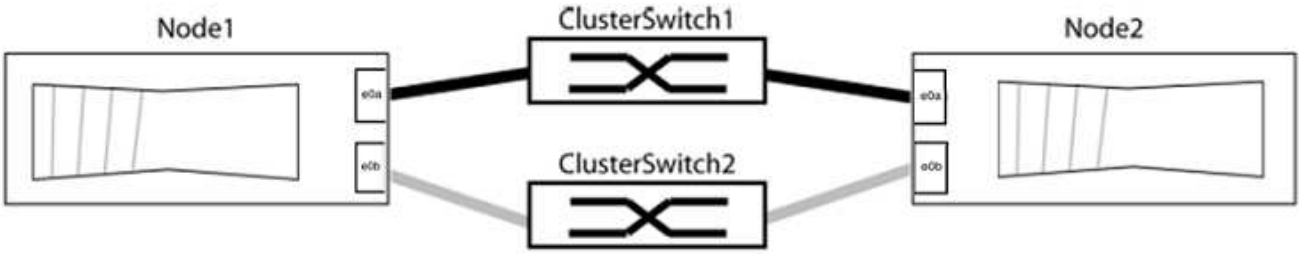
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Fase 2: Configurare le porte e il cablaggio

1. Organizzare le porte del cluster su ciascun switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano allo switch del cluster 1 e le porte del cluster nel gruppo 2 vadano allo switch2 del cluster. Questi gruppi sono richiesti più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e lo stato del collegamento:

   `network port show -ipspace Cluster`

   Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo viene identificato come "node1:e0a" e "node2:e0a" e l'altro come "node1:e0b" e "node2:e0b". I nodi potrebbero utilizzare porte cluster diverse in quanto variano in base al sistema.



   Verificare che il valore delle porte sia di `up` Per la colonna "link" e un valore di `healthy` Per la colonna "Health Status" (Stato 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 tutte le LIF del cluster si trovino sulle porte home.

   Verificare che la colonna "is-home" sia `true` Per ciascuna 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 porte home, ripristinare tali LIF alle porte home:

`network interface revert -vserver Cluster -lif *`

4. Disattivare l'autorevert per le LIF del cluster:

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

5. Verificare che tutte le porte elencate nella fase precedente siano collegate a uno switch di rete:

   `network device-discovery show -port cluster_port`

   La colonna "dispositivo rilevato" deve essere il nome dello switch del cluster a cui è collegata 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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
   ```

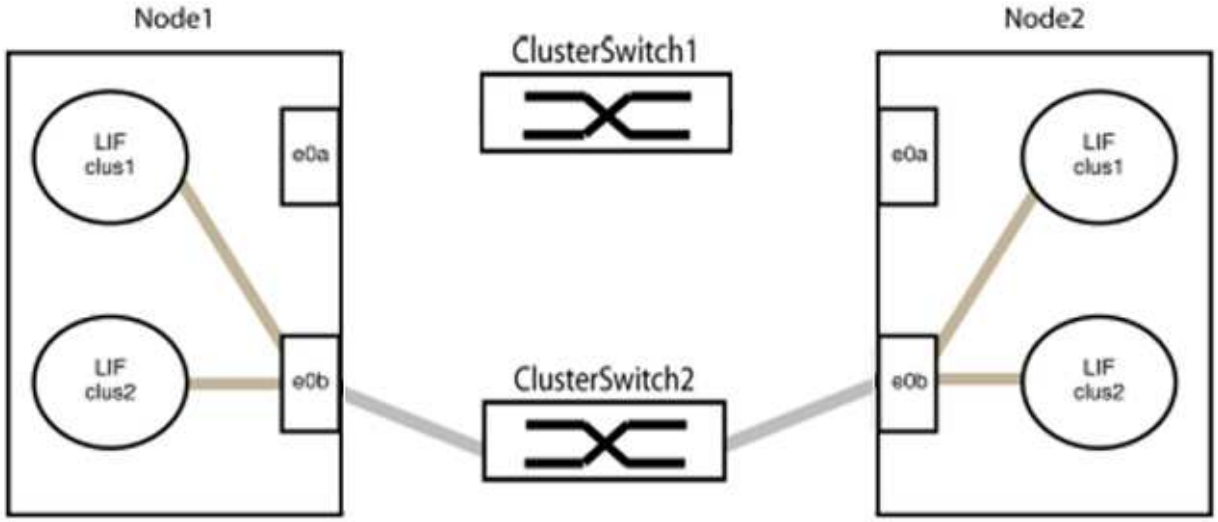
   Tutte le unità devono essere master o secondarie.

2. Impostare la configurazione senza switch per le porte del gruppo 1.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal raggruppo1 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

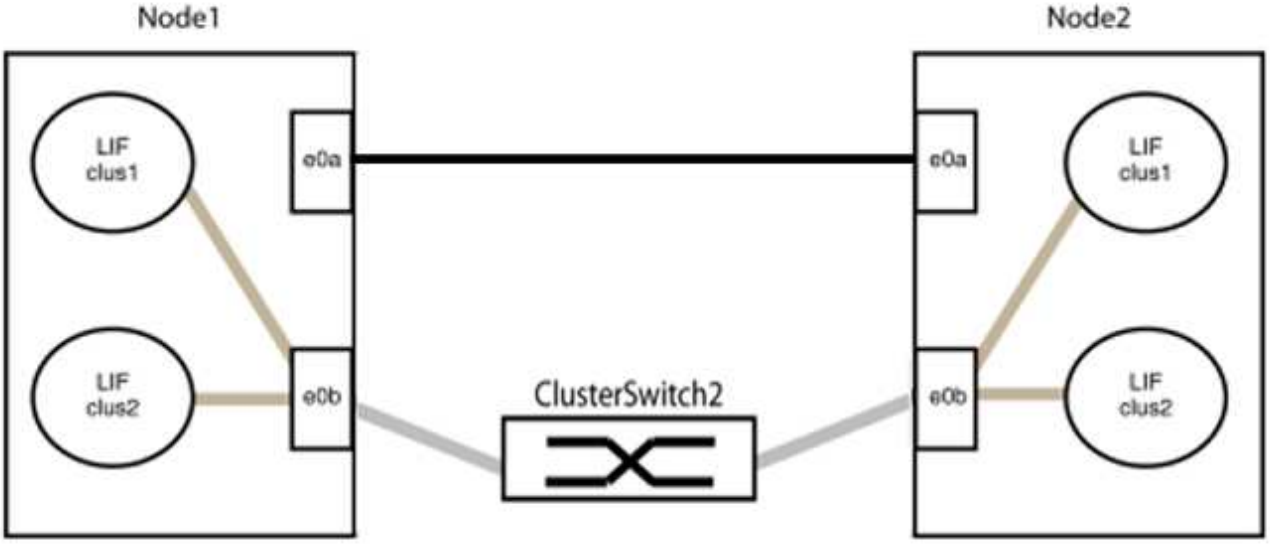
   a. Scollegare tutti i cavi dalle porte del raggruppo1 contemporaneamente.

      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 da una parte all'altro.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2:



3. L'opzione di rete del cluster senza switch passa da `false` a. `true`. Questa operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione switchless sia impostata su `true`:

`network options switchless-cluster show`

Il seguente esempio mostra che il cluster senza switch 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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)
```

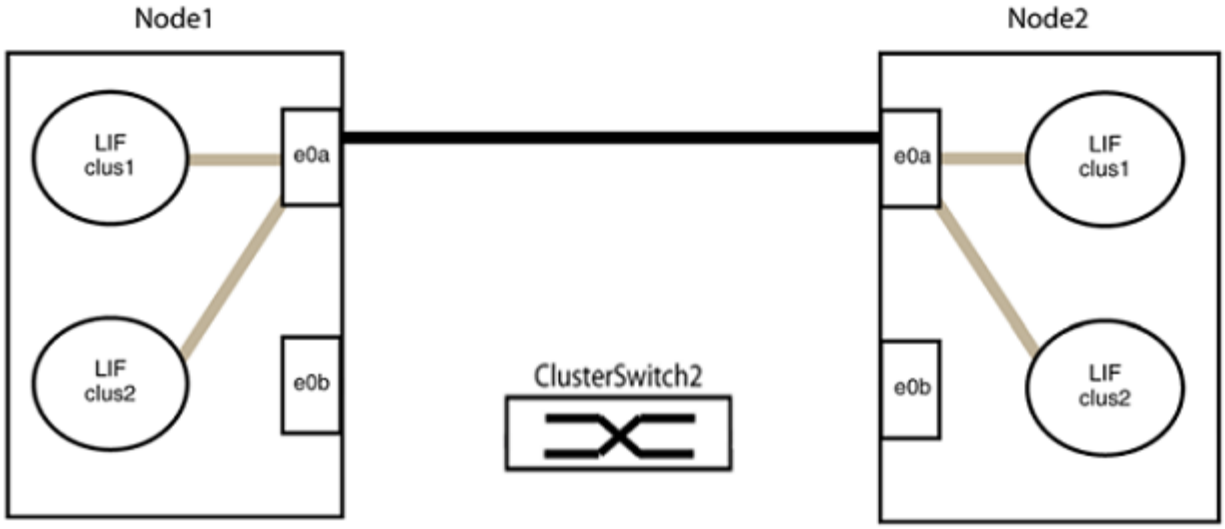
Prima di passare alla fase successiva, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

1. impostare la configurazione senza switch per le porte del gruppo 2.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

   a. Scollegare tutti i cavi dalle porte del raggruppo2 contemporaneamente.

      Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua attraverso la connessione diretta tra le porte "e0a":



b. Collegare le porte del group2 in modo che si inserano nella parte posteriore.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2 e "e0b" sul nodo 1 è collegato a "e0b" sul nodo 2:

Fase 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 collegate correttamente 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 le LIF del cluster:

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

3. Verificare che tutte le LIF siano a casa. Questa operazione potrebbe richiedere alcuni secondi.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostra esempio

I LIF sono stati ripristinati se la colonna "is Home" è `true`, come illustrato per `node1_clus2` e. `node2_clus2` nel seguente esempio:

```
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 dei cluster LIFS non è tornato alle porte home, ripristinarli 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 nodi:

   `cluster show`

   Mostra esempio

   L'esempio seguente mostra epsilon su entrambi i nodi da visualizzare `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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 è stata soppressa la creazione automatica dei casi, riattivarla richiamando un messaggio AutoSupport:

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

   Per ulteriori informazioni, vedere "Articolo della Knowledge base di NetApp 1010449: Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificate".

2. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

Quali sono le prossime novità?

Dopo aver sostituito gli interruttori, puoi "configurare il monitoraggio dello stato dello switch".

Cisco Nexus 9336C-FX2 o 9336C-FX2-T.

Inizia subito

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.

> Lo switch Ethernet Health monitor non supporta ONTAP 9.13.1P8 e versioni precedenti e 9.14.1P3 e precedenti o NX-OS 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:

- Si dispone del numero e del tipo di cavi e connettori appropriati per gli switch. Vedere "Hardware Universe".
- A seconda del tipo di switch che si sta configurando inizialmente, è necessario collegarsi alla porta della console dello switch con il cavo della console incluso.

Requisiti di rete

Sono necessarie le seguenti informazioni di rete per tutte le configurazioni dello switch.

- Subnet IP per il traffico di rete di gestione
- Nomi host e indirizzi IP per ciascuno dei controller del sistema di storage e per tutti gli switch applicabili
- La maggior parte dei controller del sistema di storage viene gestita tramite l'interfaccia e0M connettendosi alla porta di servizio Ethernet (icona chiave). Nei sistemi AFF A800 e AFF A700s, l'interfaccia e0M utilizza una porta Ethernet dedicata.
- Fare riferimento a. "Hardware Universe" per informazioni aggiornate.

Per ulteriori informazioni sulla configurazione iniziale dello switch, consultare la seguente guida: "Guida all'installazione e all'aggiornamento di 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 parte di 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, rivedere l'elenco dei componenti e dei numeri parte.

Dettagli del numero di parte

La tabella seguente elenca il numero di parte e la descrizione per gli interruttori 9336C-FX2 e 9336C-FX2-T, le ventole e gli alimentatori:

Codice del ricambio	Descrizione
X190200-CS-PE	Interruttore quadro strumenti, N9336C 36Pt PTSX 10/25/40/100g
X190200-CS-PI	Interruttore quadro strumenti, N9336C 36Pt PSIN 10/25/40/100g
X190212-CS-PE	Interruttore quadro strumenti, N9336C 12pt (9336C-FX2-T) PTSX 10/25/40/100g
X190212-CS-PI	Interruttore quadro strumenti, N9336C 12pt (9336C-FX2-T) PSIN 10/25/40/100g
SW-N9K-FX2-24P-UPG	SW, licenza POD Cisco 9336CFX2 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 di accessori X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W PSU - flusso d'aria di scarico laterale
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W PSU - flusso d'aria di aspirazione lato porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flusso d'aria di scarico lato porta
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flusso d'aria di aspirazione lato porta

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, creare un nuovo account Smart. Per ulteriori informazioni, vedere "Creare un nuovo account Smart".
2. Richiedere l'accesso a un account Smart esistente. Per ulteriori informazioni, vedere "Richiedere l'accesso a un account Smart esistente".

Una volta acquistata la licenza Smart, installare 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 degli switch Cisco Nexus serie 9000" pagina:

Titolo del documento	Descrizione
Guida all'installazione dell'hardware della serie Nexus 9000	Fornisce informazioni dettagliate sui requisiti del sito, sui dettagli dell'hardware dello switch e sulle opzioni di installazione.
Cisco Nexus 9000 Series Software Configuration Guide (scegliere la guida per la release NX-OS installata sugli switch)	Fornisce le informazioni di configurazione iniziale dello switch necessarie prima di poter configurare lo switch per il funzionamento ONTAP.
Guida all'aggiornamento e al downgrade del software per Cisco Nexus serie 9000 NX-OS (scegliere la guida per la release NX-OS installata sugli switch)	Fornisce informazioni su come eseguire il downgrade dello switch al software dello switch supportato da ONTAP, se necessario.
Cisco Nexus serie 9000 NX-OS Command Reference Master Index	Fornisce collegamenti ai vari riferimenti ai comandi forniti da Cisco.
Riferimento MIB Cisco Nexus 9000	Descrive i file MIB (Management Information base) per i centralini Nexus 9000.
Guida ai messaggi del sistema NX-OS serie Nexus 9000	Descrive i messaggi di sistema per gli switch Cisco Nexus serie 9000, quelli che sono informativi e altri che possono aiutare a diagnosticare problemi con collegamenti, hardware interno o software di sistema.
Note sulla versione di Cisco Nexus 9000 Series NX-OS (scegliere le note per la release NX-OS installata sugli switch)	Descrive le funzioni, i bug e le limitazioni di Cisco Nexus serie 9000.
Conformità alle normative e informazioni sulla sicurezza per Cisco Nexus serie 9000	Fornisce informazioni legali, sulla conformità e sulla sicurezza degli switch Nexus serie 9000 a livello internazionale.

Documentazione sui 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 release di ONTAP.
"Hardware Universe"	Fornisce informazioni sulla compatibilità e sulla configurazione dell'hardware NetApp.

Kit di guide e documentazione del cabinet

Per installare uno switch Cisco 9336-FX2 in un cabinet NetApp, consultare la seguente documentazione hardware.

Nome	Descrizione
"Cabinet di sistema 42U, guida dettagliata"	Descrive le FRU associate all'armadio 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 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:

- È necessario che sia installato 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 l'indirizzo. Questo è necessario per determinare l'origine dei messaggi ricevuti.
- Un ID CCO deve essere associato a un contratto Cisco SMARTnet Service appropriato per la tua azienda.
- Cisco SMARTnet Service deve essere disponibile per la registrazione del dispositivo.

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 esempio relativo ai cavi fornisce esempi di assegnazione delle porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che è possibile utilizzare per la configurazione del cluster.

2. **"Installare lo switch"**

Installare gli switch 9336C-FX2 e 9336C-FX2-T.

3. **"Installare lo switch in un armadio NetApp"**

Installare gli switch 9336C-FX2 e 9336C-FX2-T e il pannello pass-through in un cabinet NetApp , secondo necessità.

4. **"Analisi del cablaggio e della configurazione"**

Esaminare il supporto per le porte Ethernet NVIDIA , i requisiti FEC 25GbE e le informazioni sulle risorse TCAM.

Completare la scheda di lavoro relativa al cablaggio Cisco Nexus 9336C-FX2 o 9336C-FX2-T.

Se si desidera documentare le piattaforme supportate, scaricare un PDF di questa pagina e completare il foglio di lavoro relativo al cablaggio.

Il foglio di lavoro di esempio relativo ai cavi fornisce esempi di assegnazione delle porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che è possibile utilizzare per la configurazione del cluster.

- 9336C-FX2 esempio di foglio di lavoro per il cablaggio
- 9336C-FX2 foglio di lavoro cablaggio vuoto
- 9336C-FX2-T esempio di foglio di lavoro di cablaggio (12 porte)
- 9336C-FX2-T foglio di lavoro cablaggio vuoto (12 porte)

9336C-FX2 esempio di foglio di lavoro per il cablaggio

La definizione di porta di esempio su ciascuna coppia di switch è la seguente:

Switch del cluster A		Switch del cluster B	
Porta dello switch	Utilizzo di nodi e porte	Porta dello switch	Utilizzo di nodi e porte
1	Nodo 4 x 10 GbE 1	1	Nodo 4 x 10 GbE 1
2	Nodo 4 x 10 GbE 2	2	Nodo 4 x 10 GbE 2
3	Nodo 4 x 10 GbE 3	3	Nodo 4 x 10 GbE 3
4	Nodo 4 x 25 GbE 4	4	Nodo 4 x 25 GbE 4
5	Nodo 4 x 25 GbE 5	5	Nodo 4 x 25 GbE 5
6	Nodo 4 x 25 GbE 6	6	Nodo 4 x 25 GbE 6
7	40/100GbE nodo 7	7	40/100GbE nodo 7
8	40/100GbE nodo 8	8	40/100GbE nodo 8
9	40/100GbE nodo 9	9	40/100GbE nodo 9
10	40/100GbE nodo 10	10	40/100GbE nodo 10
11	40/100GbE nodo 11	11	40/100GbE nodo 11
12	40/100GbE nodo 12	12	40/100GbE nodo 12
13	40/100GbE nodo 13	13	40/100GbE nodo 13
14	40/100GbE nodo 14	14	40/100GbE nodo 14
15	40/100GbE nodo 15	15	40/100GbE nodo 15
16	40/100GbE nodo 16	16	40/100GbE nodo 16
17	40/100GbE nodo 17	17	40/100GbE nodo 17
18	40/100GbE nodo 18	18	40/100GbE nodo 18
19	40/100GbE nodo 19	19	40/100GbE nodo 19
20	40/100GbE nodo 20	20	40/100GbE nodo 20
21	40/100GbE nodo 21	21	40/100GbE nodo 21

Switch del cluster A		Switch del cluster B	
22	40/100GbE nodo 22	22	40/100GbE nodo 22
23	40/100GbE nodo 23	23	40/100GbE nodo 23
24	40/100GbE nodo 24	24	40/100GbE nodo 24
da 25 a 34	Riservato	da 25 a 34	Riservato
35	100GbE ISL alla porta B dello switch 35	35	100GbE ISL per commutare Una porta 35
36	100GbE ISL alla porta B dello switch 36	36	100GbE ISL per commutare Una porta 36

9336C-FX2 foglio di lavoro cablaggio vuoto

È possibile utilizzare il foglio di lavoro dei cavi vuoto per documentare le piattaforme supportate come nodi in un cluster. La sezione *connessioni cluster supportate* di "Hardware Universe" definisce le porte del cluster utilizzate dalla piattaforma.

Switch del cluster A		Switch 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	

Switch del cluster A		Switch del cluster B	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
da 25 a 34	Riservato	da 25 a 34	Riservato
35	100GbE ISL alla porta B dello switch 35	35	100GbE ISL per commutare Una porta 35
36	100GbE ISL alla porta B dello switch 36	36	100GbE ISL per commutare Una porta 36

9336C-FX2-T esempio di foglio di lavoro di cablaggio (12 porte)

La definizione di porta di esempio su ciascuna coppia di switch è la seguente:

Switch del cluster A		Switch del cluster B	
Porta dello switch	Utilizzo di nodi e porte	Porta dello switch	Utilizzo di nodi e porte
1	Nodo 4 x 10 GbE 1	1	Nodo 4 x 10 GbE 1
2	Nodo 4 x 10 GbE 2	2	Nodo 4 x 10 GbE 2

Switch del cluster A		Switch del cluster B	
3	Nodo 4 x 10 GbE 3	3	Nodo 4 x 10 GbE 3
4	Nodo 4 x 25 GbE 4	4	Nodo 4 x 25 GbE 4
5	Nodo 4 x 25 GbE 5	5	Nodo 4 x 25 GbE 5
6	Nodo 4 x 25 GbE 6	6	Nodo 4 x 25 GbE 6
7	40/100GbE nodo 7	7	40/100GbE nodo 7
8	40/100GbE nodo 8	8	40/100GbE nodo 8
9	40/100GbE nodo 9	9	40/100GbE nodo 9
10	40/100GbE nodo 10	10	40/100GbE nodo 10
da 11 a 34	Richiede licenza	da 11 a 34	Richiede licenza
35	100GbE ISL alla porta B dello switch 35	35	100GbE ISL per commutare Una porta 35
36	100GbE ISL alla porta B dello switch 36	36	100GbE ISL per commutare Una porta 36

9336C-FX2-T foglio di lavoro cablaggio vuoto (12 porte)

È possibile utilizzare il foglio di lavoro dei cavi vuoto per documentare le piattaforme supportate come nodi in un cluster. La sezione *connessioni cluster supportate* di "Hardware Universe" definisce le porte del cluster utilizzate dalla piattaforma.

Switch del cluster A		Switch del cluster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	

Switch del cluster A		Switch del cluster B	
7		7	
8		8	
9		9	
10		10	
da 11 a 34	Richiede licenza	da 11 a 34	Richiede licenza
35	100GbE ISL alla porta B dello switch 35	35	100GbE ISL per commutare Una porta 35
36	100GbE ISL alla porta B dello switch 36	36	100GbE ISL per commutare Una porta 36

Vedere "Hardware Universe" per ulteriori 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

Assicurarsi di disporre di quanto segue:

- Accesso a un server HTTP, FTP o TFTP nel sito di installazione per scaricare le release 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 per il cablaggio".
- RCF di rete cluster e rete di gestione NetApp applicabili scaricati dal NetApp Support Site all'indirizzo "mysupport.netapp.com". Tutti gli switch della rete cluster e di gestione Cisco vengono forniti con la configurazione standard predefinita di fabbrica di Cisco. Questi switch hanno anche la versione corrente del software NX-OS, ma non hanno gli RCF caricati.
- "Documentazione richiesta su switch e ONTAP".

Fasi

1. Rack di switch e controller della rete di gestione e della rete del cluster.

Se si sta installando…	Quindi…
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 il pannello pass-through in un cabinet NetApp.
Apparecchiatura in un rack Telco	Consultare le procedure fornite nelle guide all'installazione dell'hardware dello switch e le istruzioni di installazione e configurazione di NetApp.

2. Collegare gli switch della rete cluster e della rete di gestione ai controller utilizzando i fogli di lavoro di cablaggio completi.
3. Accendere la rete del cluster e gli switch e i controller della rete di gestione.

Quali sono le prossime novità?

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

Assicurarsi di disporre di quanto segue:

- Il kit pannello pass-through, disponibile presso NetApp (codice X8784-R6).

  Il kit di pannelli pass-through NetApp contiene il seguente hardware:

  - Un pannello di chiusura pass-through
  - Quattro viti 10-32 x 0,75
  - Quattro dadi a clip da 10-32
- Per ogni switch, otto viti da 10-32 o 12-24 e dadi a clip per montare le staffe e le guide di scorrimento sui montanti anteriori e posteriori dell'armadio.
- 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 devono essere inclusi con gli switch. Se non sono stati forniti con gli switch, è possibile ordinarli presso NetApp (codice X1558A-R6).

- Per i requisiti di preparazione iniziale, il contenuto del kit e le precauzioni di sicurezza, vedere "Guida all'installazione dell'hardware di Cisco Nexus serie 9000".

Fasi

1. Installare il pannello di chiusura pass-through nel cabinet NetApp.

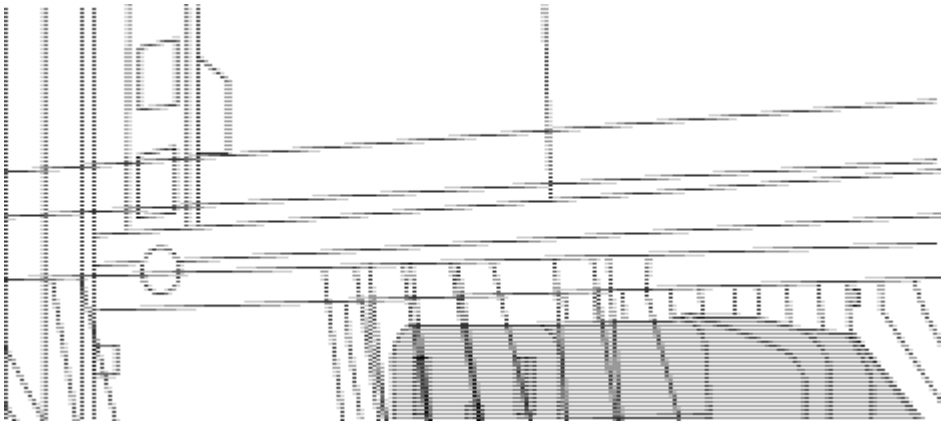
   a. Determinare la posizione verticale degli interruttori e del pannello di chiusura nell'armadio.

In questa procedura, il pannello di chiusura viene installato in U40.

b. Installare due dadi a clip su ciascun lato nei fori quadrati appropriati per le guide anteriori dell'armadio.

c. Centrare il pannello verticalmente per evitare l'ingresso nello spazio rack adiacente, quindi serrare le viti.

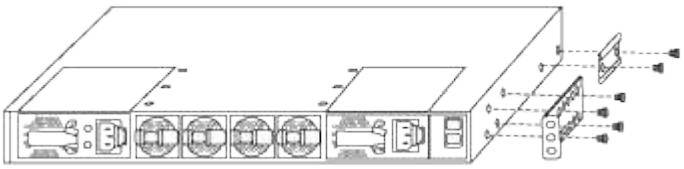
d. Inserire i connettori femmina di entrambi i cavi di collegamento da 48 pollici dalla parte posteriore del pannello e attraverso il gruppo spazzole.



(1) connettore femmina del cavo di collegamento.

2. Installare le staffe per il montaggio in rack sullo chassis dello switch Nexus 9336C-FX2.

a. Posizionare una staffa anteriore per il montaggio su rack su un lato dello chassis dello switch in modo che l'orecchio di montaggio sia allineato con la piastra anteriore dello chassis (lato alimentatore o ventola), quindi utilizzare quattro viti M4 per fissare la staffa allo chassis.

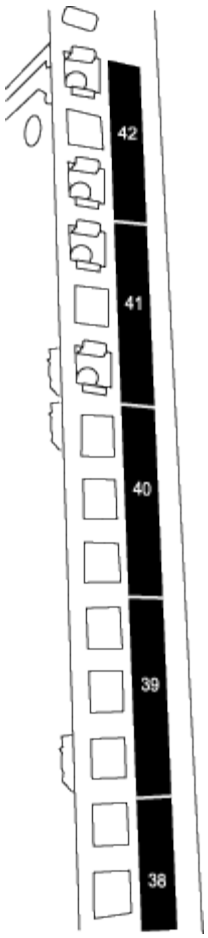


b. Ripetere il passaggio 2a con l'altra staffa anteriore per il montaggio su rack sull'altro lato dello switch.

c. Installare la staffa per il montaggio su rack posteriore sul telaio dello switch.

d. Ripetere il punto 2c con l'altra staffa posteriore per il montaggio su rack sull'altro lato dello switch.

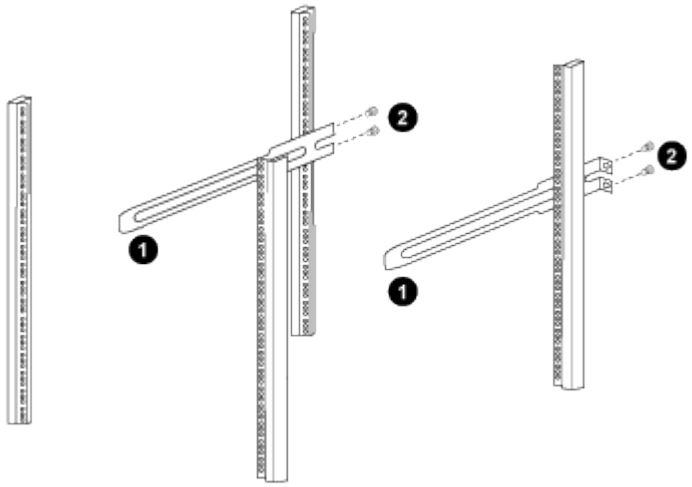
3. Montare i dadi a clip nelle posizioni dei fori quadrati per tutti e quattro i montanti IEA.



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 di scorrimento nel cabinet.

   a. Posizionare la prima guida scorrevole in corrispondenza del contrassegno RU42 sul lato posteriore del montante posteriore sinistro, inserire le viti con il tipo di filettatura corrispondente, quindi serrare le viti con le dita.



(1) mentre si fa scorrere delicatamente la guida scorrevole, allinearla ai fori delle viti nel rack.

(2) serrare le viti delle guide di scorrimento ai montanti dell'armadietto.

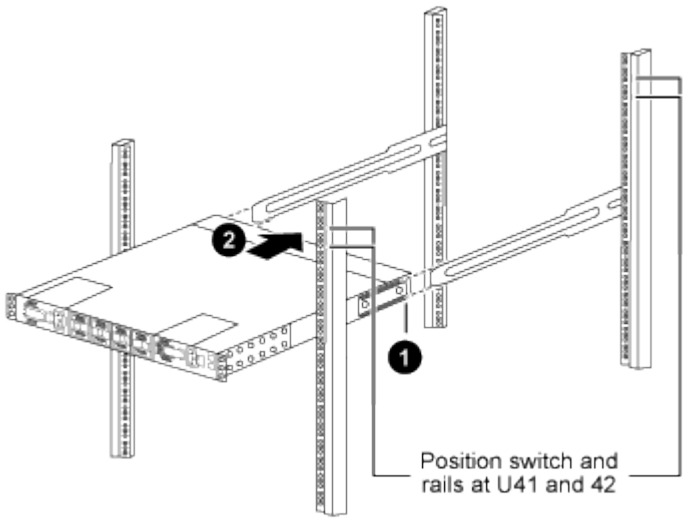
a. Ripetere il passaggio 4a per il montante posteriore destro.

b. Ripetere i passaggi 4a e 4b nelle posizioni RU41 dell'armadio.

5. Installare lo switch nell'armadio.

> Questa fase richiede due persone: Una per supportare lo switch dalla parte anteriore e un'altra per guidare lo switch nelle guide di scorrimento posteriori.

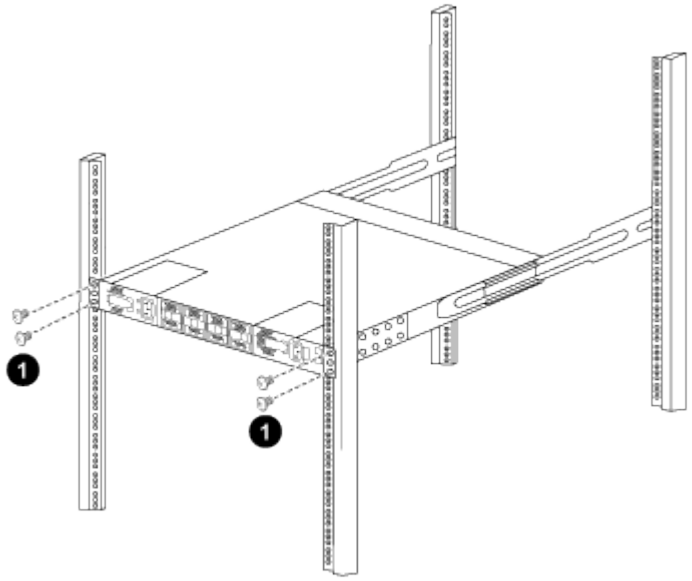
a. Posizionare la parte posteriore dell'interruttore su RU41.



(1) quando lo chassis viene spinto verso i montanti posteriori, allineare le due guide posteriori per il montaggio su rack con le guide di scorrimento.

(2) far scorrere delicatamente lo switch fino a quando le staffe anteriori per il montaggio su rack non sono a filo con i montanti anteriori.

b. Collegare lo switch al cabinet.



(1) con una persona che tiene la parte anteriore del telaio a livello, l'altra deve serrare completamente le quattro viti posteriori ai montanti del cabinet.

a. Con il telaio ora supportato senza assistenza, serrare completamente le viti anteriori sui montanti.

b. Ripetere i passi da 5a a 5c per il secondo switch nella posizione RU42.

> Utilizzando lo switch completamente installato come supporto, non è necessario tenere la parte anteriore del secondo switch durante il processo di installazione.

6. Una volta installati gli switch, collegare i cavi di collegamento alle prese di alimentazione dello switch.
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 diverse PDU.

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. Il cavo CAT6 per ogni switch deve essere instradato attraverso il pannello pass-through dopo l'installazione degli switch per connettersi agli switch di gestione o alla rete di gestione.

Quali sono le prossime novità?

Dopo aver installato gli switch nell'armadio NetApp , è possibile"configurare gli switch Cisco Nexus 9336C-FX2 e 9336C-FX2-T" .

Esaminare le considerazioni relative al cablaggio e alla configurazione

Prima di configurare gli switch 9336C-FX2 e 9336C-FX2-T, leggere le seguenti considerazioni.

Supporto di porte Ethernet NVIDIA CX6, CX6-DX e CX7 GB

Se si collega una porta dello switch a un controller ONTAP utilizzando le porte NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7) NIC, 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
```

Vedere "Hardware Universe" per ulteriori informazioni sulle porte dello switch.

25GbE requisiti FEC

Porte da e0b GbE/FAS2820 e0a

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.

Consultare l'articolo della Knowledge base "Le porte non si collegano su Cisco Nexus 9336C-FX2 a causa delle risorse TCAM" per ulteriori informazioni 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 lo switch"**
   Configurare gli switch cluster 9336C-FX2 e 9336C-FX2-T.

2. **"Preparare l'installazione del software NX-OS e di 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. **"Installare o aggiornare 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 **"Verificare 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

Assicurarsi di disporre di quanto segue:

- Accesso a un server HTTP, FTP o TFTP nel sito di installazione per scaricare le release 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 per il cablaggio".
- RCF di rete cluster e rete di gestione NetApp applicabili scaricati dal NetApp Support Site all'indirizzo "mysupport.netapp.com". Tutti gli switch della rete cluster e di gestione Cisco vengono forniti con la configurazione standard predefinita di fabbrica di Cisco. Questi switch hanno anche la versione corrente del software NX-OS, ma non hanno gli RCF caricati.
- "Documentazione richiesta su switch e ONTAP".

Fasi

1. Eseguire una configurazione iniziale degli switch di rete del cluster.

   Fornire le risposte appropriate alle seguenti domande iniziali di configurazione al primo avvio dello switch. La policy di sicurezza del sito definisce le risposte e i servizi da abilitare.

Prompt	Risposta
Interrompere il provisioning automatico e continuare con la normale configurazione? (sì/no)	Rispondere con **sì**. Il valore predefinito è no
Applicare lo standard di password sicura? (sì/no)	Rispondere con **sì**. L'impostazione predefinita è sì.
Inserire la password per admin.	La password predefinita è "admin"; è necessario creare una nuova password complessa. Una password debole può essere rifiutata.

Prompt	Risposta
Accedere alla finestra di dialogo della configurazione di base? (sì/no)	Rispondere con **yes** alla configurazione iniziale dello switch.
Creare un altro account di accesso? (sì/no)	La risposta dipende dalle policy del sito relative agli amministratori alternativi. L'impostazione predefinita è **NO**.
Configurare la stringa di comunità SNMP di sola lettura? (sì/no)	Rispondere con **no**. Il valore predefinito è no
Configurare la stringa di comunità SNMP in lettura/scrittura? (sì/no)	Rispondere con **no**. Il valore predefinito è no
Inserire il nome dello switch.	Inserire il nome dello switch, che può contenere al massimo 63 caratteri alfanumerici.
Continuare con la configurazione di gestione out-of-band (mgmt0)? (sì/no)	Rispondere con **yes** (impostazione predefinita) al prompt. Al prompt mgmt0 IPv4 address: (Indirizzo IPv4: Mgmt0), immettere l'indirizzo IP IP: ip_address (Indirizzo_ip).
Configurare il gateway predefinito? (sì/no)	Rispondere con **sì**. Al prompt dell'indirizzo IPv4 del gateway predefinito, immettere default_gateway.
Configurare le opzioni IP avanzate? (sì/no)	Rispondere con **no**. Il valore predefinito è no
Abilitare il servizio telnet? (sì/no)	Rispondere con **no**. Il valore predefinito è no
Servizio SSH abilitato? (sì/no)	Rispondere con **sì**. L'impostazione predefinita è sì. SSH è consigliato quando si utilizza Ethernet Switch Health Monitor (CSHM) per le funzioni di raccolta dei log. SSHv2 è consigliato anche per una maggiore sicurezza.
Inserire il tipo di chiave SSH che si desidera generare (dsa/rsa/rsa1).	L'impostazione predefinita è **rsa**.
Inserire il numero di bit della chiave (1024-2048).	Inserire il numero di bit della chiave compreso tra 1024 e 2048.
Configurare il server NTP? (sì/no)	Rispondere con **no**. Il valore predefinito è no
Configurare il livello di interfaccia predefinito (L3/L2)	Rispondi con **L2**. L'impostazione predefinita è L2.

Prompt	Risposta
Configurare lo stato di interfaccia della porta dello switch predefinito (shut/noshut)	Rispondere con **noshut**. L'impostazione predefinita è noshut.
Configurare il profilo di sistema Copp (rigido/moderato/lenient/denso)	Rispondere con **Strict**. L'impostazione predefinita è rigorosa.
Modificare la configurazione? (sì/no)	A questo punto, viene visualizzata la nuova configurazione. Esaminare e apportare le modifiche necessarie alla configurazione appena inserita. Rispondere con **no** al prompt se si è soddisfatti della configurazione. Rispondere con **yes** se si desidera modificare le impostazioni di configurazione.
Utilizzare questa configurazione e salvarla? (sì/no)	Rispondere con **yes** per salvare la configurazione. In questo modo vengono aggiornate automaticamente le immagini del sistema e del kickstart. Se non si salva la configurazione in questa fase, nessuna delle modifiche sarà effettiva al successivo riavvio dello switch.

2. Verificare le opzioni di configurazione effettuate sul display visualizzato al termine dell'installazione e assicurarsi di salvare la configurazione.
3. Controllare la versione degli switch di rete del cluster e, se necessario, scaricare la versione del software supportata da NetApp sugli switch da "Download del software Cisco" pagina.

Quali sono le prossime novità?

Dopo aver configurato gli switch, puoi "prepararsi a installare il software NX-OS e RCF".

Preparare l'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 consigliata

- "Pagina switch Ethernet Cisco"

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

- "Guide all'aggiornamento e al downgrade del software"

  Per la documentazione completa sulle procedure di aggiornamento e di downgrade degli switch Cisco, consultare le guide appropriate per il software e l'aggiornamento disponibili sul sito Web di Cisco.

- "Upgrade di 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, selezionare **Disruptive Upgrade** (aggiornamento distruttivo) e selezionare la release corrente e la release di destinazione dall'elenco a discesa.

A proposito degli esempi

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

- I nomi dei due switch Cisco sono cs1 e cs2.
- I nomi dei nodi sono cluster1-01 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::*>` prompt indica il nome del cluster.

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 9000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

Fasi

1. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

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

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

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato (`*>`).

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

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

Mostra esempio

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
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. Visualizzare gli attributi della porta di rete:

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

Mostra esempio

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

Node: cluster1-02
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Visualizzare le informazioni sui LIF:

```
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      169.254.209.69/16
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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  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
```

Tutte le release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. verifica che il comando di indirizzamento automatico sia abilitato in tutte le LIF del cluster:

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

Quali sono le prossime novità?

Dopo esserti preparato per installare il software NX-OS e RCF, puoi "installare o aggiornare il software NX-OS".

Installare o aggiornare 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 descritta in "Preparazione all'installazione di NX-OS e RCF".

Verifica dei requisiti

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

Documentazione consigliata

- "Pagina switch Ethernet Cisco"

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

- "Guide all'aggiornamento e al downgrade del software"

  Per la documentazione completa sulle procedure di aggiornamento e di downgrade degli switch Cisco, consultare le guide appropriate per il software e l'aggiornamento disponibili sul sito Web di Cisco.

- "Upgrade di Cisco Nexus 9000 e 3000 e matrice ISSU"

  Fornisce informazioni su Disruptive Upgrade/Downgrade del software Cisco NX-OS sugli switch della serie Nexus 9000

in base alle release attuali e a quelle di destinazione.

Nella pagina, selezionare **Disruptive Upgrade** (aggiornamento distruttivo) e selezionare la release corrente e la release di destinazione dall'elenco a discesa.

A proposito degli esempi

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

- I nomi dei due switch Cisco sono cs1 e cs2.
- I nomi dei nodi sono cluster1-01, cluster1-02, cluster1-03 e cluster1-04.
- I nomi LIF del cluster sono cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2 , cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1 e cluster1-04_clus2.
- Il `cluster1::*>` prompt indica il nome del cluster.

Installare il software

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 9000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

Fasi

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

   ```
   network device-discovery show
   ```

Mostra esempio

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

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

   a. Verificare che tutte le porte del cluster siano **up** con uno stato integro:

      `network port show -role cluster`

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

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

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

Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

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

5. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

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

6. Copia il software NX-OS e le immagini EPLD sullo switch Nexus 9336C-FX2.

Mostra esempio

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

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


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

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

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

   ```
   show version
   ```

Mostra esempio

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


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

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

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Installare l’immagine NX-OS.

   L’installazione del file immagine ne provoca il caricamento 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
   ```

Mostra esempio

```
cs2# show version

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

Software
  BIOS: version 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, accedere nuovamente 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 funzionanti in tutti i nodi del cluster:

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

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

Ignore
                                                          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 dello switch dal cluster.

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

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

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

2 entries were displayed.
```

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

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

13. Verificare che il cluster funzioni correttamente:

    `cluster show`

    Mostra esempio

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

14. Ripetere i passaggi da 6 a 13 per installare il software NX-OS sullo switch CS1.
15. Abilitare il ripristino automatico sulle LIF del cluster.

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

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

In caso di mancato ritorno delle LIF del cluster alle porte home, puoi ripristinarle manualmente dal nodo locale:

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

Quali sono le prossime novità?

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

Installare o aggiornare la panoramica 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.

Per ulteriori informazioni sull'installazione o l'aggiornamento di RCF, consultare l'articolo della Knowledge base"Come cancellare la configurazione su uno switch Cisco Interconnect mantenendo la connettività remota".

Configurazioni RCF disponibili

Nella tabella seguente sono descritti gli RCF disponibili per diverse configurazioni. Scegliere l'RCF applicabile alla propria configurazione.

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

Nome RCF	Descrizione
2 cluster-ha-breakout	Supporta due cluster ONTAP con almeno otto nodi, compresi i nodi che utilizzano porte ha e cluster condivisi.
4 cluster-ha-breakout	Supporta quattro cluster ONTAP con almeno quattro nodi, inclusi i nodi che utilizzano porte ha e cluster condivisi.
1-Cluster-ha	Tutte le porte sono configurate per 40 GbE/100GbE GbE. Supporta il traffico ha/cluster 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 ha/cluster condiviso sulle porte per i nodi che utilizzano porte ha/cluster condivisi: Sistemi AFF A320, AFF A250 e FAS500f. Inoltre, tutte le porte possono essere utilizzate come porte cluster dedicate.
Storage ha-cluster	Le porte sono configurate per 40/100GbE GbE per Cluster+ha, 4x10GbE breakout per il cluster e 4x25GbE breakout per Cluster+ha e 100GbE GbE per ogni coppia ha storage.
Cluster	Due versioni di RCF con diverse allocazioni di 4 porte 10 GbE (breakout) e porte 40/100GbE. Tutti i nodi FAS/AFF sono supportati, ad eccezione dei sistemi AFF A320, AFF A250 e FAS500f.
Storage	Tutte le porte sono configurate per connessioni storage NVMe da 100GbE GB.

Documentazione consigliata

- "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 esistere dipendenze di comando tra la sintassi di comando nell'RCF

e la sintassi trovata nelle versioni specifiche di NX-OS.

- "Switch Cisco Nexus serie 3000"

  Per la documentazione completa sulle procedure di aggiornamento e di downgrade degli switch Cisco, consultare le guide appropriate per il software e l'aggiornamento disponibili sul sito Web di Cisco.

A proposito degli esempi

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

- I nomi dei due switch Cisco sono **CS1** e **CS2**.
- I nomi dei nodi sono **cluster1-01**, **cluster1-02**, **cluster1-03** e **cluster1-04**.
- I nomi LIF del cluster sono **cluster1-01_clus1**, **cluster1-01_clus2**, **cluster1-03_clus2**, **cluster1-03_clus1**, **cluster1-02_clus2**, **cluster1-02_clus1**, **cluster1-04_clus1** e **cluster1-04_clus2**.
- Il `cluster1::*>` prompt indica il nome del cluster.

Gli esempi di questa procedura utilizzano quattro nodi. Questi nodi utilizzano due porte di interconnessione cluster 10GbE **e0a** e **e0b**. Consultare "Hardware Universe" per verificare le porte cluster corrette sulle piattaforme.

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

Per informazioni dettagliate sulle configurazioni RCF disponibili, vedere "Workflow di installazione del software".

Comandi utilizzati

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 9000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato.

Quali sono le prossime novità?

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

Installazione 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).

Prima di iniziare

Verificare le seguenti installazioni e connessioni:

- Collegamento della console allo switch. Il collegamento alla console è opzionale se si dispone dell'accesso remoto allo switch.
- Lo switch CS1 e lo switch CS2 sono accesi e la configurazione iniziale dello switch è completa (l'indirizzo IP di gestione e SSH è impostato).
- È stata installata la versione NX-OS desiderata.
- Le connessioni ISL tra gli switch sono collegate.
- Le porte del cluster di nodi ONTAP non sono connesse.

Fase 1: Installare l'RCF sugli interruttori

1. Accedere allo switch CS1 usando SSH o usando una console seriale.
2. Copiare l'RCF nella memoria di avvio 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"Cisco Nexus 9000 Series NX-OS Command Reference" guide.

   Mostra esempio

   Questo esempio mostra l'utilizzo di TFTP per copiare un RCF nel bootflash dello 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"Cisco Nexus 9000 Series NX-OS Command Reference" guide.

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

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

4. Esaminare l'output dello striscione da `show banner motd` comando. Leggere e seguire queste istruzioni per garantire la corretta configurazione e il corretto funzionamento dello switch.

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

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

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

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 Cisco Interconnect 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. Emettere il `write erase` comando 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
    ```

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

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

13. Riavviare l'interruttore CS1.

    ```
    cs1# reload

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

14. Ripetere i passaggi da 1 a 13 sullo switch cs2.
15. Collegare le porte del cluster di tutti i nodi nel cluster ONTAP agli switch CS1 e CS2.

Fase 2: Verificare i collegamenti dello switch

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

    `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    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
```

```
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         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
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
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     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           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 dettagliate sull'utilizzo di porte e VLAN specifiche, fare riferimento alla sezione banner e note importanti nell'RCF.

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

```
show port-channel summary
```

Mostra esempio

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

Fase 3: Configurare il cluster ONTAP

NetApp consiglia di utilizzare System Manager per configurare nuovi cluster.

System Manager offre un workflow semplice e facile per la configurazione e la configurazione del cluster, che include l'assegnazione di un indirizzo IP di gestione dei nodi, l'inizializzazione del cluster, la creazione di un Tier locale, la configurazione dei protocolli e il provisioning dello storage iniziale.

Passare a. "Configurare ONTAP su un nuovo cluster con Gestione di sistema" per le istruzioni di installazione.

Quali sono le prossime novità?

Dopo aver installato l'RCF, puoi "verificare la configurazione SSH".

Aggiornamento del file di configurazione di riferimento (RCF)

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- RCF corrente.
- Se si sta aggiornando la versione RCF, è necessaria una configurazione di avvio nell'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 RCF in modo che venga creata un'istanza della versione corretta in caso di riavvio futuro.

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

Prima di installare una nuova versione del software dello switch e gli RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Prima di cancellare le impostazioni dello switch, è necessario essere collegati allo switch utilizzando la console seriale o aver conservato le informazioni di configurazione di base.

Passaggio 1: Preparazione per l'aggiornamento

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

```
network device-discovery show
```

Mostra esempio

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       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 ciascuna porta del cluster.

   a. Verificare che tutte le porte del cluster siano **up** con uno stato integro:

      `network port show -role cluster`

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

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

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

Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90    N9K-
C9336C
     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. Disattiva l'autorevert sulle LIF del cluster.

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

Fase 2: Configurare le porte

1. Sullo switch del cluster cs1, spegnere 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 collegate per evitare problemi di connessione di rete. Per "Nodo fuori dal quorum quando si esegue la migrazione della LIF del cluster durante l'aggiornamento del sistema operativo dello switch" ulteriori informazioni, consultare l'articolo della Knowledge base.

2. Verifica che le LIF del cluster abbiano eseguito il failover sulle porte ospitate nello switch del cluster CS1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   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 funzioni correttamente:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

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

   `show running-config`

   a. Registrare eventuali aggiunte personalizzate tra l'attuale `running-config` e il file RCF in uso (ad esempio una configurazione SNMP per la tua organizzazione).

   b. 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 Cisco Interconnect 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. Utilizzare 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. Riavviare lo switch:

    ```
    switch# reload

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

11. Dopo 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 nella memoria di avvio 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"Cisco Nexus 9000 Series NX-OS Command Reference" guide.

    Questo esempio mostra l'utilizzo di TFTP per copiare un RCF nel bootflash dello 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"Cisco Nexus 9000 Series NX-OS Command Reference" .

Questo esempio mostra il file RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` in fase di installazione sull'interruttore 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 si controlla l'output per verificare che l'RCF sia corretto, assicurarsi che le seguenti informazioni siano corrette:

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

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

15. Riapplicare le eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a "Esaminare le considerazioni relative al cablaggio e alla configurazione" per i dettagli su eventuali ulteriori modifiche necessarie.
16. Dopo aver verificato che le versioni di RCF, le aggiunte personalizzate e le impostazioni dello switch siano corrette, copiare il file running-config nel file startup-config.

    Per ulteriori informazioni sui comandi Cisco , consultare la guida appropriata nel"Cisco Nexus 9000 Series NX-OS Command Reference" .

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

    [] 100% Copy complete
    ```

17. Riavviare l'interruttore CS1. È possibile ignorare gli avvisi "`cluster switch Health monitor'" e gli eventi "`cluster ports down'" riportati 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 funzionanti in tutti i nodi del cluster:

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

Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

Ignore
                                                          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 dello switch dal cluster.

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

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       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                      Type               Address
Model
--------------------------- ------------------ ---------------
-----
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, sulla console dello switch cs1 potrebbero essere presenti i seguenti output:

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

19. Verificare che il cluster funzioni correttamente:

    `cluster show`

    Mostra esempio

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

20. Ripetere i passaggi da 1 a 19 sullo switch cs2.
21. Abilitare il ripristino automatico sulle LIF del cluster.

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

Fase 3: Verificare la configurazione della rete cluster e lo stato del cluster

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

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

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
```

```
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
Eth1/34
33   VLAN0033                         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
34   VLAN0034                         active    Eth1/23, Eth1/24,
Eth1/25
                                                  Eth1/26, Eth1/27,
Eth1/28
                                                  Eth1/29, Eth1/30,
Eth1/31
                                                  Eth1/32, Eth1/33,
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     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           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 dettagliate sull'utilizzo di porte e VLAN specifiche, fare riferimento alla sezione banner e note importanti nell'RCF.

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

```
show port-channel summary
```

Mostra esempio

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)        Eth1/36(P)
cs1#
```

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

   `network interface show -role cluster`

Mostra esempio

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

In caso di mancato ritorno delle LIF del cluster alle porte home, puoi ripristinarle manualmente dal nodo locale:

```
network interface revert -vserver vserver_name -lif lif_name
```

6. Verificare che il cluster funzioni correttamente:

```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------- -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
4 entries were displayed.
cluster1::*>
```

7. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  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
```

Tutte le release di ONTAP

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

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

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

Quali sono le prossime novità?

Dopo aver aggiornato il tuo RCF, puoi"verificare la configurazione SSH" .

Verificare la configurazione DELLA SSH

Se si utilizzano le funzioni di Ethernet Switch Health Monitor (CSHM) e di raccolta dei log,

verificare che le chiavi SSH e SSH siano attivate sugli switch del cluster.

Fasi

1. Verificare che SSH sia attivato:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verificare che le chiavi SSH siano attivate:

```
show ssh key
```

Mostra esempio

```
(switch)# show ssh key

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

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

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

Quando si attiva FIPS, è necessario cambiare il conteggio dei bit a 256 sullo switch utilizzando il comando `ssh key ecdsa 256 force`. Per ulteriori informazioni, vedere "Configurare la sicurezza di rete utilizzando FIPS".

Quali sono le prossime novità?

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.

A proposito di questa attività

- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

Fasi

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.

Verifica dei requisiti

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 del cluster:

- NetApp CN1610
- Cisco 9336C-FX2
- Cisco 9336C-FX2-T

Per informazioni dettagliate sulle porte supportate e sulle relative configurazioni, consultare "Hardware Universe".

Di cosa hai bisogno

Verificare che la configurazione soddisfi i seguenti requisiti:

- Il cluster esistente è configurato e funziona correttamente.
- Tutte le porte del cluster sono nello stato **up** 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 presenta quanto segue:
  - Un cluster NetApp ridondante e completamente funzionale che utilizza switch NetApp CN1610.
  - Connettività di gestione e accesso alla console sia per gli switch CN1610 NetApp che per i nuovi switch.
  - Tutte le LIF del cluster in stato up con le LIF del cluster si trovano sulle 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

A proposito degli esempi

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

- Gli switch del 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* rispettivamente sul nodo 2.
- Il `cluster1::*>` prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono *e3a* e *e3b*.

A proposito di questa attività

Questa procedura riguarda il seguente scenario:

- L'interruttore C2 viene sostituito per primo dall'interruttore CS2.

- Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - Tutte le LIF del cluster eseguono il failover sul nuovo switch CS2.
- Il cablaggio tra i nodi e C2 viene quindi scollegato da C2 e ricollegato a CS2.

- L'interruttore C1 è sostituito dall'interruttore CS1.
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
    - Tutte le LIF del cluster 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 interswitch operativo (ISL). Ciò è dovuto alla progettazione, in quanto le modifiche alla versione di RCF possono influire temporaneamente sulla connettività ISL. Per garantire le operazioni senza interruzioni del cluster, viene eseguita la seguente procedura per il failover di tutte le LIF del cluster allo switch partner operativo, eseguendo al tempo stesso la procedura sullo switch target.

Fase 1: Preparazione per la migrazione

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

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

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

3. Disattiva l'autorevert sulle LIF del cluster.

   Disabilitando l'opzione di auto-revert per questa procedura, le LIF del cluster non torneranno automaticamente alla porta home. Rimangono sulla porta corrente mentre continua ad essere attiva e operativa.

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

Fase 2: Configurare le porte e il cablaggio

1. Determinare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.

   Ogni porta deve essere visualizzata per `Link` e. `healthy` per `Health Status`.

   a. Visualizzare 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
```

b. Visualizzare le informazioni relative ai LIF e ai relativi nodi principali designati:

`network interface show -vserver Cluster`

Viene visualizzato ciascun LIF `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 sono collegate agli switch del cluster esistenti nel seguente modo (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 sono collegati nel seguente modo (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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3a
node2                 Eth1/2        124    H           AFF-A400
e3a
C2                    0/13          179    S I s       CN1610
0/13
C2                    0/14          175    S I s       CN1610
0/14
C2                    0/15          179    S I s       CN1610
0/15
C2                    0/16          175    S I s       CN1610
0/16

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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
C1                    0/13          175    S I s       CN1610
0/13
C1                    0/14          175    S I s       CN1610
0/14
C1                    0/15          175    S I s       CN1610
0/15
C1                    0/16          175    S I s       CN1610
0/16
```

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 collegate alle porte del cluster dei nodi per eseguire il failover delle LIF del cluster.

   Non tentare di migrare manualmente le 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. Visualizzare 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 seguente modo, dal punto di vista dei nodi:

   `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
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 di nodi siano in funzione:

   `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
```

6. Sullo switch C1, chiudere le porte collegate alle porte del cluster dei nodi per eseguire il failover delle 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 essere visualizzata `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 seguente modo, dal punto di vista dei nodi:

   `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    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 in funzione:

    `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 dispongano di una connessione a ciascuno 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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster:

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

2. Verificare che tutte le LIF della rete del cluster siano nuovamente presenti sulle porte domestiche:

   ```
   network interface show
   ```

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
```

3. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

4. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

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.

Verifica dei requisiti

Assicurarsi che:

- Il numero di serie dello switch è stato verificato per garantire la migrazione dello switch corretto.
- Alcune porte degli switch Nexus 9336C-FX2 sono configurate per funzionare a 10 GbE o 40 GbE.
- La connettività 10 GbE e 40 GbE dai nodi agli switch del cluster Nexus 9336C-FX2 è stata pianificata, migrata e documentata.
- Il cluster funziona correttamente (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.
  - Prima di eseguire la migrazione delle LIF ai nuovi switch, verifica che i file di configurazione di riferimento (RCF) siano stati applicati correttamente a tutti i nuovi switch.
  - Controllare le configurazioni in esecuzione e di avvio su entrambi gli switch prima di modificare il traffico di rete.
  - Qualsiasi personalizzazione del sito, ad esempio DNS, NTP, SMTP, SNMP, E SSH, sono configurati sui nuovi switch.
- È possibile accedere alla tabella di compatibilità degli switch in "Switch Ethernet Cisco" Per le versioni supportate di ONTAP, NX-OS e RCF.
- Sono state esaminate le guide all'aggiornamento e al software appropriate disponibili sul sito Web di Cisco per le procedure di aggiornamento e downgrade dello switch Cisco all'indirizzo "Supporto degli switch Cisco Nexus serie 9000" pagina.

> Se si modifica la velocità delle porte del cluster e0a e E1a nei sistemi AFF A800 o AFF C800, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug 1570339" E l'articolo della Knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

Migrare gli switch

A proposito degli esempi

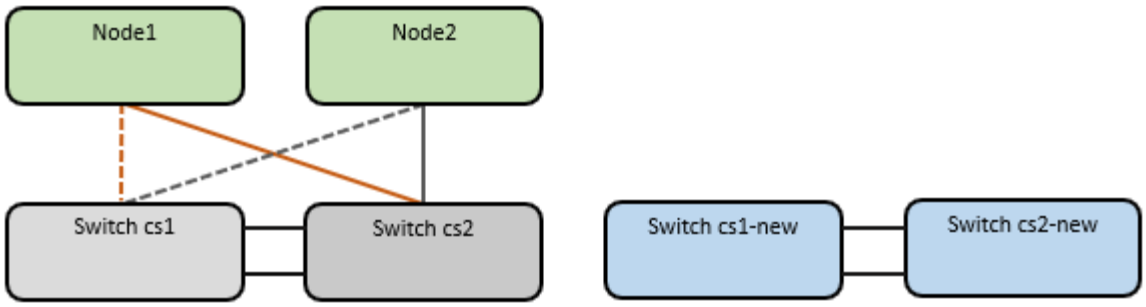
Gli esempi di questa procedura utilizzano due nodi. Questi nodi utilizzano due porte di interconnessione cluster 10GbE e0a e e0b. Vedere "Hardware Universe" per verificare le porte cluster corrette sulle piattaforme.

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

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

- I nomi dei due switch Cisco esistenti sono **cs1** e **cs2**
- I nuovi switch in 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:



A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e. "Switch Nexus serie 9000" Comandi; vengono utilizzati i comandi ONTAP, se non diversamente indicato.

Questa procedura riguarda il seguente scenario:

- L'interruttore CS2 viene sostituito dall'interruttore CS2-nuovo per primo.
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
    - Tutte le LIF del cluster 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.
- L'interruttore CS1 viene sostituito dall'interruttore CS1-nuovo.
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
    - Tutte le 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 interswitch operativo (ISL). Ciò è dovuto alla progettazione, in quanto le modifiche alla versione di RCF possono influire temporaneamente sulla connettività ISL. Per garantire le operazioni senza interruzioni del cluster, viene eseguita la seguente procedura per il failover di tutte le LIF del cluster allo switch partner operativo, eseguendo al tempo stesso la procedura sullo switch target.

Fase 1: Preparazione per la migrazione

1. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

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

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

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

```
set -privilege advanced
```

Viene visualizzato il prompt Advanced (*>).

Fase 2: Configurare le porte e il 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. Visualizzare 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 ciascuna porta del cluster.

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

      `network port show -ipspace Cluster`

Mostra esempio

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

Node: 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
```

b. Verificare che tutte le interfacce del cluster (LIFF) si trovino sulle 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
```

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    10.233.205.92    N5K-
C5596UP
      Serial Number: FOXXXXXXXGS
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP

cs2                         cluster-network     10.233.205.93   N5K-
C5596UP
      Serial Number: FOXXXXXXXGD
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP
```

4. Disattiva il ripristino automatico sulle LIF del cluster.

   Disabilitando l'opzione di auto-revert per questa procedura, le LIF del cluster non torneranno automaticamente alla porta home. Rimangono sulla porta corrente mentre continua ad essere attiva e operativa.

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

   > La disattivazione dell'indirizzamento automatico garantisce che ONTAP esegua il failover delle LIF del cluster solo in caso di arresto delle porte dello switch.

5. Sullo switch del cluster CS2, chiudere le porte collegate alle porte del cluster di **tutti** i nodi per eseguire il failover delle 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. Verifica che le LIF del cluster abbiano eseguito il failover sulle porte ospitate nello switch del cluster CS1. Questa operazione potrebbe richiedere alcuni secondi.

   `network interface show -vserver Cluster`

   Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------ ----------
------- ----
Cluster
            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 funzioni correttamente:

   `cluster show`

   Mostra esempio

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

8. Se le LIF del cluster sono state sostituite con lo switch CS1 e il cluster è integro, passare al Fase. 10. Se alcune LIF del cluster non sono sane o il cluster non è integro, puoi ripristinare la connettività allo switch CS2, come segue:

   a. Visualizzare le porte collegate 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. Verifica che le LIF del cluster abbiano eseguito il failover sulle porte ospitate nello switch del cluster CS1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
---------- ------- ----
Cluster
            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 funzioni correttamente:

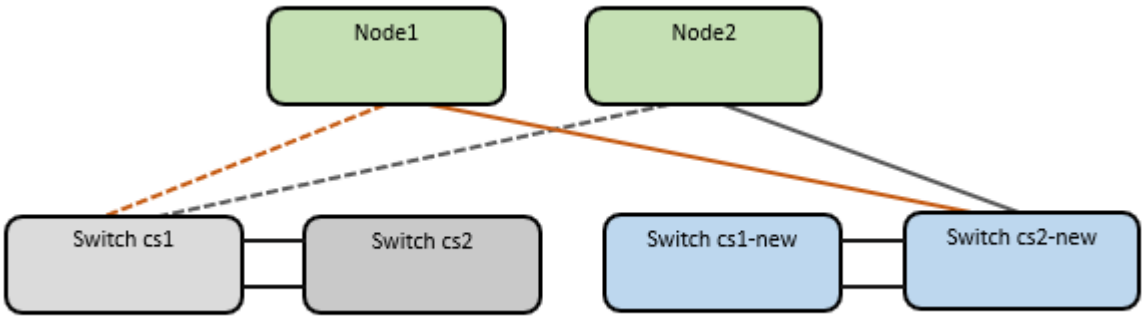
```
cluster show
```

Mostra esempio

```
cluster1::*> cluster show
Node       Health  Eligibility   Epsilon
---------- ------- ------------- -------
node1      true    true          false
node2      true    true          false
```

9. Dopo aver ripristinato lo stato della LIF e del cluster, riavviare il processo da Fase. 4.
10. spostare tutti i cavi di collegamento del nodo del cluster dal vecchio switch CS2 al nuovo switch CS2.

I cavi di connessione del nodo del cluster sono stati spostati nel nuovo switch cs2



11. Verificare lo stato delle connessioni di rete trasferite a cs2-New:

```
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 spostate devono essere in alto.

12. Controllare le informazioni 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
----------- ------ ------------------------- -------------
--------------
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 il neighbor.

13. Confermare i collegamenti della porta 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 collegate alle porte del cluster di **tutti** i nodi per eseguire il failover delle 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#
```

Tutte le LIF del cluster eseguono il failover sullo switch da CS2 nuovi.

15. Verificare che le LIF del cluster abbiano eseguito il failover alle porte ospitate nello switch CS2-new. Questa operazione potrebbe richiedere alcuni secondi:

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     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 funzioni correttamente:

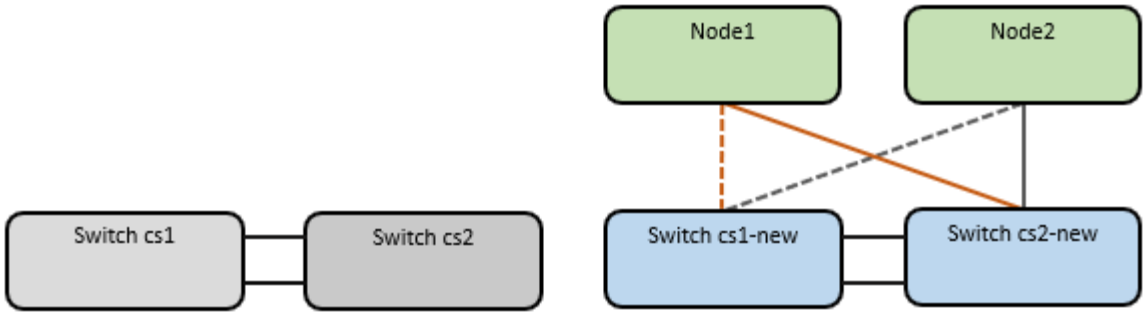
    `cluster show`

    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 del cluster da cs1 al nuovo switch cs1-new.

    I cavi di connessione del nodo del cluster sono stati spostati nel nuovo switch cs1



18. Verificare lo stato delle connessioni di rete trasferite a cs1-New:

```
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 spostate devono essere in alto.

19. Controllare le informazioni 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 il neighbor.

20. Confermare i collegamenti della porta 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)
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster.

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

2. Verificare che le LIF del cluster siano ripristinate alle porte home (questa operazione potrebbe richiedere un minuto):

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

Se le LIF del cluster non sono tornate alla porta home, ripristinarle manualmente:

```
network interface revert -vserver Cluster -lif *
```

3. Verificare che il cluster funzioni correttamente:

```
cluster show
```

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source          Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 è stata soppressa la creazione automatica dei casi, riattivarla richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=END`

Quali sono le prossime novità?

Dopo aver migrato gli switch, puoi"configurare il monitoraggio dello stato dello switch" .

Migrare a un cluster con switch 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 10GB BASE-T integrate per le porte di rete del cluster.

Verifica dei requisiti

Di cosa hai bisogno

- Per la configurazione senza switch a due nodi:
  - La configurazione senza switch a due nodi è configurata e funziona correttamente.

- Tutte le porte del cluster si trovano nello stato **up**.
- Tutte le interfacce logiche del cluster (LIFF) si trovano nello stato **up** e nelle porte home.
- Vedere "Hardware Universe" Per tutte le versioni di ONTAP supportate.

- Per la configurazione dello switch Cisco Nexus 9336C-FX2:
  - Entrambi gli switch dispongono di connettività di rete di gestione.
  - Gli switch del cluster sono accessibili dalla console.
  - Le connessioni switch nodo-nodo e switch-to-switch Nexus 9336C-FX2 utilizzano cavi Twinax o in fibra.

    Vedere "Hardware Universe" per ulteriori informazioni sul cablaggio.
- I cavi ISL (Inter-Switch link) 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, ad esempio SMTP, SNMP e SSH, viene configurata sui nuovi switch.

A proposito degli esempi

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

- I nomi degli switch 9336C-FX2 sono cs1 e cs2.
- I nomi delle SVM del cluster sono node1 e node2.
- I nomi delle LIF sono rispettivamente node1_clus1 e node1_clus2 sul nodo 1 e node2_clus1 e node2_clus2 sul nodo 2.
- Il `cluster1::*>` prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono e0a e e0b.

Vedere "Hardware Universe" per informazioni sulle porte del cluster per le piattaforme in uso.

Migrare gli switch

Fase 1: Preparazione per la migrazione

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

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

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

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

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

   ```
   set -privilege advanced
   ```

Il prompt avanzato (`*>`).

Fase 2: Configurare le porte e il cablaggio

1. Disattivare tutte le porte rivolte ai nodi (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 rivolte al nodo da 1 a 34 sono disattivate 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 le porte ISL e fisiche dell'ISL tra i due switch 9336C-FX2 cs1 e cs2 siano installate sulle porte 1/35 e 1/36:

   ```
   show port-channel summary
   ```

Mostra esempio

L'esempio seguente mostra che le porte ISL sono installate 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 installate 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. Visualizzare l'elenco dei dispositivi vicini:

`show cdp neighbors`

Questo comando fornisce informazioni sui dispositivi collegati al sistema.

Mostra esempio

Nell'esempio riportato di seguito sono elencati 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
```

Nell'esempio riportato di seguito sono elencati 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 installate:

   `network port show -ipspace Cluster`

   Ogni porta deve essere visualizzata per `Link` e sano per `Health Status`.

   Mostra esempio

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

Node: node1

                                                  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: node2

                                                  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.
```

5. Verificare che tutte le LIF del cluster siano operative:

   `network interface show -vserver Cluster`

   Viene visualizzato ciascun LIF del cluster `true` per `Is Home` e hanno un `Status Admin/Oper` di up/up.

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. Verificare che l'autorevert sia attivato su tutte le LIF del cluster:

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

Mostra esempio

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. Scollegare il cavo dalla porta del cluster e0a sul nodo 1, quindi collegare e0a alla porta 1 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.

Il "Hardware Universe - Switch" contiene ulteriori informazioni sul cablaggio.

"Hardware Universe - Switch"

8. Scollegare il cavo dalla porta del cluster e0a sul nodo 2, quindi collegare e0a alla porta 2 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.
9. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs1.

Mostra esempio

L'esempio seguente mostra che le porte da 1/1 a 1/34 sono attivate 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 tutte le LIF del cluster siano funzionanti, operative e visualizzate come `true` per `Is Home`:

`network interface show -vserver Cluster`

Mostra esempio

L'esempio seguente mostra che tutte le LIF sono in su su node1 e node2 e questo `Is Home` i risultati sono veri:

```
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.
```

11. Visualizza informazioni sullo stato dei nodi nel cluster:

    `cluster show`

Mostra esempio

Nell'esempio seguente vengono visualizzate informazioni sullo stato 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 del cluster e0b sul nodo 1, quindi collegare e0b alla porta 1 sullo switch del

cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.

13. Scollegare il cavo dalla porta del cluster e0b sul nodo 2, quindi collegare e0b alla porta 2 sullo switch del cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch 9336C-FX2.
14. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs2.

    Mostra esempio

    L'esempio seguente mostra che le porte da 1/1 a 1/34 sono attivate 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 installate:

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

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono 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.
```

Fase 3: Verificare la configurazione

1. Verificare che tutte le interfacce visualizzino true per `Is Home`:

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

   Il completamento di questa operazione potrebbe richiedere alcuni minuti.

Mostra esempio

L'esempio seguente mostra che tutte le LIF sono in su su node1 e node2 e questo `Is Home` i risultati sono veri:

```
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.
```

2. Verificare che entrambi i nodi dispongano di una connessione a ciascuno 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          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
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: 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         133    H           FAS2980
e0b
node2              Eth1/2         133    H           FAS2980
e0b
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Visualizzare le informazioni relative ai dispositivi di rete rilevati nel 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.
```

4. Verificare che le impostazioni siano disattivate:

```
network options switchless-cluster show
```

> Il completamento del comando potrebbe richiedere alcuni minuti. Attendere l'annuncio "3 minuti di scadenza".

Mostra esempio

L'output falso nell'esempio seguente mostra che le impostazioni di configurazione sono disattivate:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

5. Verificare lo stato dei membri del nodo nel cluster:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra informazioni sullo stato e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show

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

6. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. riportare il livello di privilegio ad admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

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).

Verifica dei requisiti

Prima di sostituire lo switch, assicurarsi che:

- È stato verificato il numero di serie dello switch per assicurarsi che venga sostituito l'interruttore corretto.
- Sul cluster e sull'infrastruttura di rete esistenti:
  - Il cluster esistente viene verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
  - Tutte le porte del cluster sono **up**.
  - Tutte le interfacce logiche del cluster (LIFF) sono **up** e sulle porte home.
  - ONTAP `cluster ping-cluster -node node1` Il comando deve indicare che la connettività di base e le comunicazioni di dimensioni superiori a quelle di PMTU hanno esito positivo su tutti i percorsi.
- Sullo switch sostitutivo Nexus 9336C-FX2:
  - La connettività di rete di gestione sullo switch sostitutivo è funzionale.
  - L'accesso della console allo switch sostitutivo è in posizione.
  - Le connessioni dei nodi sono le porte da 1/1 a 1/34.
  - Tutte le porte ISL (Inter-Switch link) sono disattivate sulle porte 1/35 e 1/36.
  - Il file di configurazione di riferimento desiderato (RCF) e lo switch dell'immagine del sistema operativo NX-OS vengono caricati sullo switch.
  - La personalizzazione iniziale dello switch è completa, come descritto in "Configurare lo switch del cluster 9336C-FX2".

    Tutte le personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengono copiate nel nuovo switch.
- È stato eseguito il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.

Attivare la registrazione della console

NetApp consiglia vivamente di attivare la registrazione della console sui dispositivi in uso e di eseguire le seguenti operazioni quando si sostituisce lo switch:

- Lasciare attivato AutoSupport durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione del caso per tutta la durata della manutenzione. Consultare questo articolo della Knowledge base "SU92: Come eliminare la creazione automatica dei casi durante le finestre di manutenzione programmata" per ulteriori dettagli.
- Attivare la registrazione della sessione per qualsiasi sessione CLI. Per istruzioni su come attivare 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 lo switch

A proposito degli esempi

Gli esempi di 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 e 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:*>

A proposito di questa attività

La seguente procedura si basa sulla seguente topologia di rete del 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/       Local  Discovered
Protocol    Port   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          Local Intrfce  Hldtme Capability  Platform      Port
ID
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(FDO220329V5)   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 per la sostituzione

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

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

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

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

2. Installare l'RCF e l'immagine appropriati sullo switch, newcs2, ed eseguire le operazioni necessarie per la preparazione del sito.

   Se necessario, verificare, scaricare e installare le versioni appropriate del software RCF e NX-OS per il nuovo switch. Se il nuovo switch è stato configurato correttamente e non sono necessari aggiornamenti per il software RCF e NX-OS, passare alla fase 2.

   a. Accedere alla *pagina Descrizione del file di configurazione di riferimento per gli switch di rete di gestione e cluster NetApp* sul sito del supporto NetApp.
   b. Fare clic sul link per la *matrice di compatibilità della rete di gestione e di rete del cluster*, quindi annotare la versione del software dello switch richiesta.
   c. Fare clic sulla freccia indietro del browser per tornare alla pagina Descrizione, fare clic su **CONTINUA**, accettare il contratto di licenza e accedere alla pagina Download.
   d. Seguire la procedura riportata nella pagina di download per scaricare i file RCF e NX-OS corretti per la versione del software ONTAP che si sta installando.

3. Sul nuovo switch, accedere come admin e chiudere tutte le porte che verranno collegate alle interfacce del cluster di nodi (porte da 1/1 a 1/34).

Se lo switch che si sta sostituendo non funziona e viene spento, passare alla fase 4. Le LIF sui nodi del cluster dovrebbero essere già riuscite a eseguire 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 tutte le LIF del cluster abbiano attivato l'autorevert:

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

   Mostra 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

4 entries were displayed.
```

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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)
```

Fase 2: Configurazione di cavi e porte

1. Spegnere le porte ISL 1/35 e 1/36 dello 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 dello switch Nexus C9336C-FX2 newcs2.
3. Richiamare le porte ISL 1/35 e 1/36 tra gli switch cs1 e newcs2, quindi verificare lo stato di funzionamento del canale della porta.

   Port-Channel deve indicare PO1(su) e Member Ports deve indicare eth1/35(P) e eth1/36(P).

Mostra esempio

Questo esempio abilita le porte ISL 1/35 e 1/36 e visualizza il riepilogo del canale delle porte 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 a quanto segue:

```
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/auto   -
false

4 entries were displayed.
```

5. Sullo stesso nodo utilizzato nella fase precedente, ripristinare la LIF del cluster associata alla porta nella fase precedente utilizzando il comando di revert dell'interfaccia di rete.

Mostra esempio

In questo esempio, LIF node1_clus2 su node1 viene invertito correttamente se il valore Home è true e la porta è e0b.

I seguenti comandi restituiscono LIF `node1_clus2` acceso `node1` alla porta home `e0a` E visualizza le 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 mostra le assegnazioni di porta corrette, in questo esempio `e0a` e. `e0b` al nodo1.

```
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. Visualizzare le informazioni sui nodi di un cluster:

`cluster show`

Mostra esempio

Questo esempio mostra che l'integrità del nodo per node1 e node2 in questo cluster è vera:

```
cluster1::*> cluster show

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

7. Verificare che tutte le porte del cluster fisico siano installate:

   `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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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)
```

Fase 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/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
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            Local Intrfce  Hldtme Capability  Platform
Port ID
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          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
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

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 cluster commutata a uno in cui due nodi sono collegati direttamente per ONTAP 9.3 e versioni successive.

Verifica dei requisiti

Linee guida

Consultare le seguenti linee guida:

- La migrazione a una configurazione cluster senza switch a due nodi è un'operazione senza interruzioni. La maggior parte dei sistemi dispone di due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per i 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 funzione 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 e utilizza ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

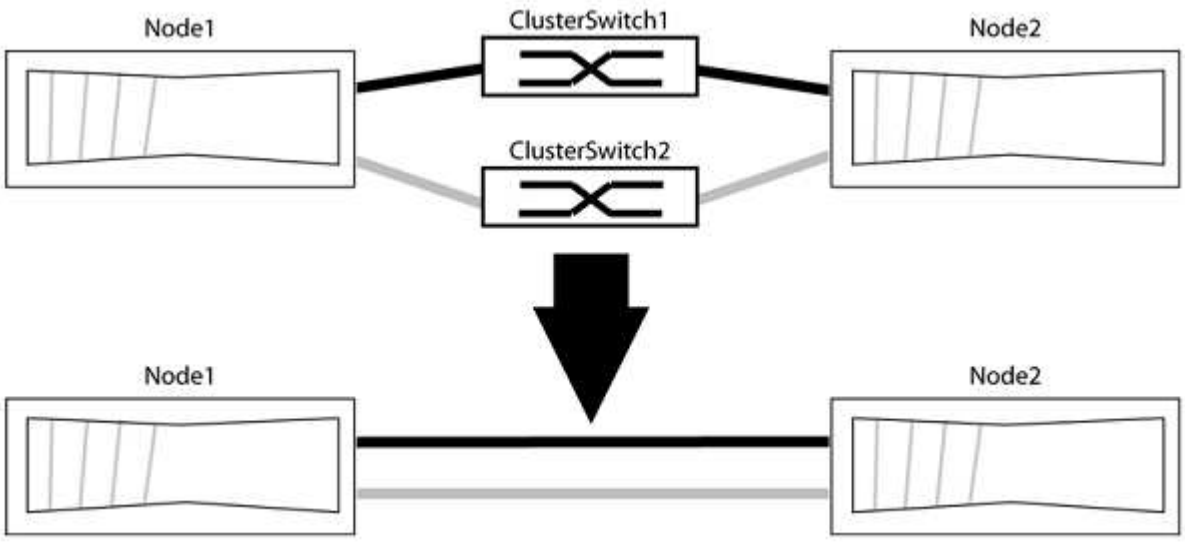
Assicurarsi di disporre di quanto segue:

- Un cluster integro costituito da due nodi collegati da switch di cluster. I nodi devono eseguire la stessa release di ONTAP.
- Ciascun nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, esistono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

A proposito di questa attività

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.



A proposito degli esempi

Gli esempi della seguente procedura mostrano i nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse in base al sistema.

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato `*>` viene visualizzato.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster senza switch, attivato per impostazione predefinita.

È possibile verificare che il rilevamento dei cluster senza switch sia attivato eseguendo il comando Advanced Privilege:

```
network options detect-switchless-cluster show
```

Mostra esempio

Il seguente esempio di output mostra se l'opzione è attivata.

```
cluster::*> network options detect-switchless-cluster show
   (network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Se "Enable Switchless Cluster Detection" (attiva rilevamento cluster senza switch) è `false`, Contattare il supporto NetApp.

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

   ```
   system node autosupport invoke -node * -type all -message
   MAINT=<number_of_hours>h
   ```

   dove `h` indica la durata della finestra di manutenzione in ore. Il messaggio informa il supporto tecnico di questa attività di manutenzione in modo che possa eliminare la creazione automatica del caso durante la finestra di manutenzione.

   Nell'esempio seguente, il comando sospende la creazione automatica del caso per due ore:

   Mostra esempio

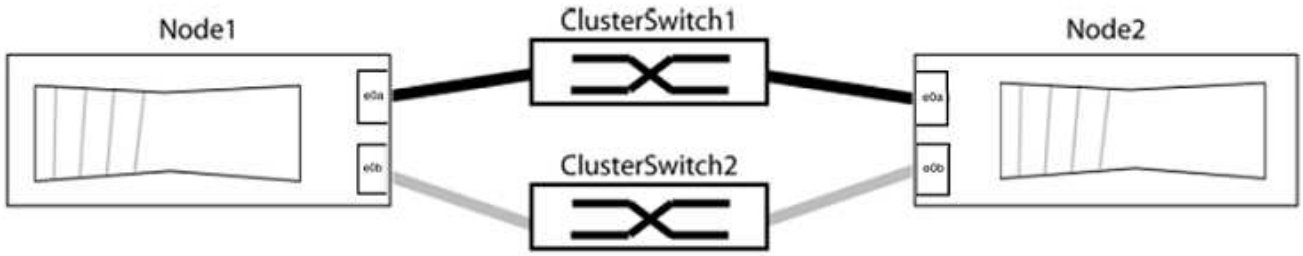
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Fase 2: Configurare le porte e il cablaggio

1. Organizzare le porte del cluster su ciascun switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano allo switch del cluster 1 e le porte del cluster nel gruppo 2 vadano allo switch2 del cluster. Questi gruppi sono richiesti più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e lo stato del collegamento:

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

   Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo viene identificato come "node1:e0a" e "node2:e0a" e l'altro come "node1:e0b" e "node2:e0b". I nodi potrebbero utilizzare porte cluster diverse in quanto variano in base al sistema.



Verificare che il valore delle porte sia di `up` Per la colonna "link" e un valore di `healthy` Per la colonna "Health Status" (Stato 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 tutte le LIF del cluster si trovino sulle porte home.

Verificare che la colonna "is-home" sia `true` Per ciascuna 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 porte home, ripristinare tali LIF alle porte home:

`network interface revert -vserver Cluster -lif *`

4. Disattivare l'autorevert per le LIF del cluster:

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

5. Verificare che tutte le porte elencate nella fase precedente siano collegate a uno switch di rete:

   `network device-discovery show -port` *`cluster_port`*

   La colonna "dispositivo rilevato" deve essere il nome dello switch del cluster a cui è collegata 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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
   ```

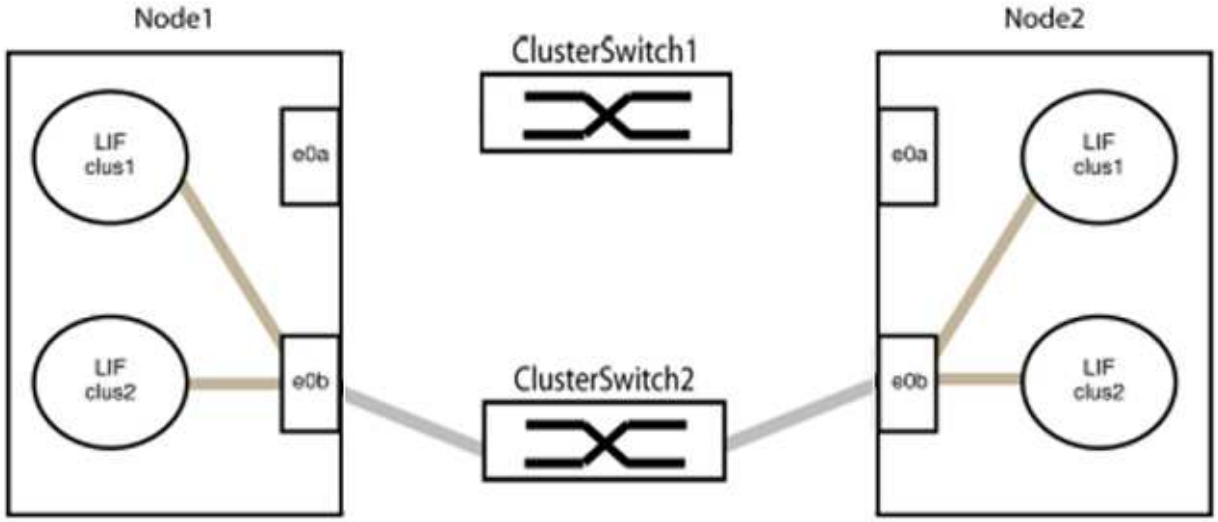
   Tutte le unità devono essere master o secondarie.

2. Impostare la configurazione senza switch per le porte del gruppo 1.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal raggruppo1 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

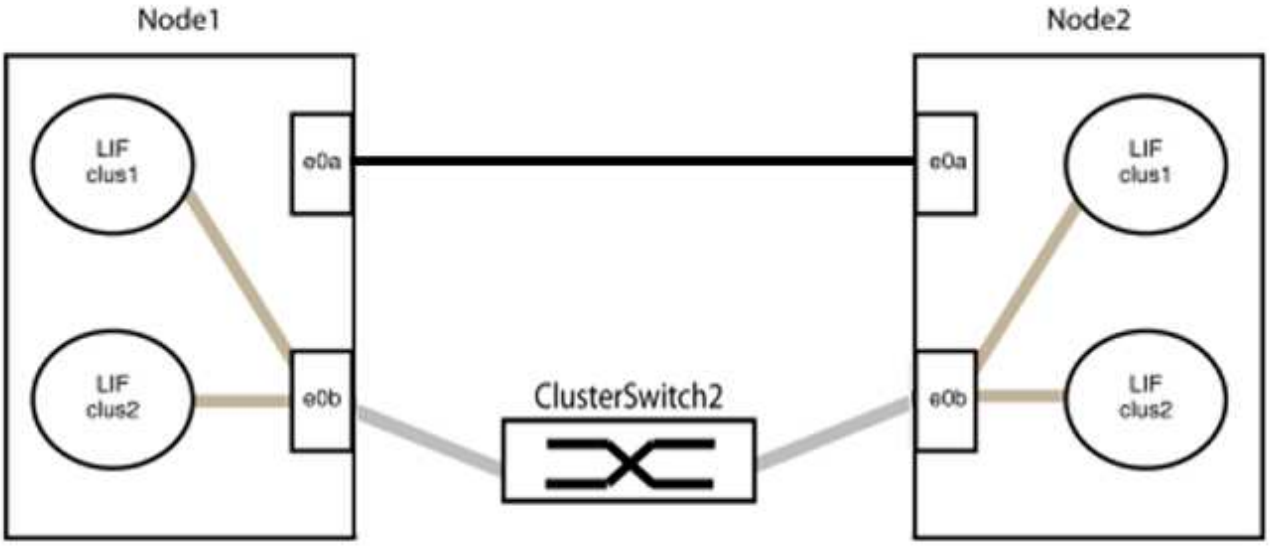
   a. Scollegare tutti i cavi dalle porte del raggruppo1 contemporaneamente.

      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 da una parte all'altro.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2:



3. L'opzione di rete del cluster senza switch passa da `false` a. `true`. Questa operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione switchless sia impostata su `true`:

`network options switchless-cluster show`

Il seguente esempio mostra che il cluster senza switch 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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)
```

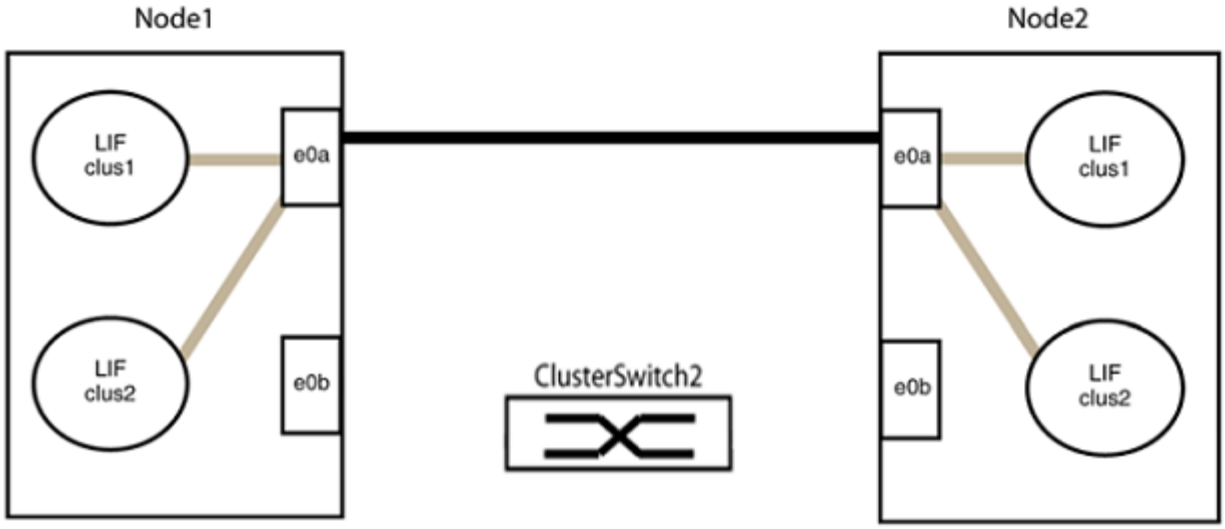
Prima di passare alla fase successiva, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

1. impostare la configurazione senza switch per le porte del gruppo 2.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

   a. Scollegare tutti i cavi dalle porte del raggruppo2 contemporaneamente.

      Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua attraverso la connessione diretta tra le porte "e0a":



b. Collegare le porte del group2 in modo che si inserano nella parte posteriore.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2 e "e0b" sul nodo 1 è collegato a "e0b" sul nodo 2:

Fase 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 collegate correttamente 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 le LIF del cluster:

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

3. Verificare che tutte le LIF siano a casa. Questa operazione potrebbe richiedere alcuni secondi.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostra esempio

I LIF sono stati ripristinati se la colonna "is Home" è `true`, come illustrato per `node1_clus2` e. `node2_clus2` nel seguente esempio:

```
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 dei cluster LIFS non è tornato alle porte home, ripristinarli 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 nodi:

   `cluster show`

   Mostra esempio

   L'esempio seguente mostra epsilon su entrambi i nodi da visualizzare `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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 è stata soppressa la creazione automatica dei casi, riattivarla richiamando un messaggio AutoSupport:

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

   Per ulteriori informazioni, vedere "Articolo della Knowledge base di NetApp 1010449: Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificate".

2. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

NVIDIA SN2100

Inizia subito

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, verificare 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, opzionali.

Lo switch NVIDIA SN2100 (X190006) viene installato nel cabinet doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Per le linee guida relative al cablaggio, vedere "Esaminare le considerazioni relative al cablaggio e alla configurazione".

Supporto di ONTAP e Linux

Lo switch NVIDIA SN2100 è uno switch 10/25/40/100GbE con Cumulus Linux. Lo switch supporta quanto segue:

- ONTAP 9.10.1P3 e versioni successive

  Lo switch SN2100 serve cluster e applicazioni di storage in ONTAP 9.10.1P3 e versioni successive su diverse coppie di switch.

- Versioni del sistema operativo Cumulus Linux (CL)

- Le versioni CL specifiche sono qualificate e supportate da NetApp. Per informazioni aggiornate sulla compatibilità, vedere la "Informazioni sugli switch Ethernet NVIDIA" pagina o la "NetApp Hardware Universe".
- Per scaricare il software SN2100 Cumulus da NVIDIA, è necessario disporre delle credenziali di accesso per accedere al portale di supporto di NVIDIA Enterprise. Consultare l'articolo della Knowledge base "Come registrarsi con NVIDIA per Enterprise Support Portal Access" .

- È possibile installare Cumulus Linux quando lo switch esegue Cumulus Linux o ONIE.

Quali sono le prossime novità?

Dopo aver esaminato i requisiti di configurazione, puoi confermare il tuo "componenti e numeri di parte".

Componenti e codici ricambio per switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, consultare l'elenco dei componenti e i codici del cabinet e del kit di guide.

Dettagli del cabinet

Lo switch NVIDIA SN2100 (X190006) viene installato nel cabinet doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Dettagli del kit ferroviario

La seguente tabella elenca il codice e la descrizione degli switch e dei kit di guide SN2100:

Codice del ricambio	Descrizione
X190006-PE	Switch cluster, NVIDIA SN2100, 16 PUNTI 100GbE, PTSX
X190006-PI	Switch cluster, NVIDIA SN2100, 16 PUNTI 100GbE, PSIN
X-MTEF-KIT-D	Kit di guide, NVIDIA Dual Switch fianco a fianco
X-MTEF-KIT-E	Kit di guide, NVIDIA Single Switch a breve profondità

Consultare la documentazione NVIDIA per ulteriori informazioni su "Installazione dello switch SN2100 e del kit guida".

Quali sono le prossime novità?

Dopo aver confermato i componenti e i numeri di parte, puoi rivedere il "documentazione richiesta".

Requisiti della documentazione per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, consultare tutta la documentazione consigliata.

Titolo	Descrizione
"Guida all'installazione dello switch NVIDIA"	Descrive come installare gli switch NVIDIA SN2100.
"NS224 NVMe Drive Shelf Cabining Guide"	Panoramica e illustrazioni che mostrano come configurare il cablaggio per gli shelf di dischi.
"NetApp Hardware Universe"	Consente di confermare l'hardware supportato, ad esempio switch e cavi storage, 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 relative al cablaggio e alla configurazione"**

Esaminare i requisiti per le connessioni ottiche, l'adattatore QSA e la velocità di switchport.

3. **"Cablare gli shelf NS224"**

Seguire le procedure di cablaggio se si dispone di un sistema in cui gli shelf di dischi 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, consultare la documentazione di NVIDIA.

Fasi

1. Esaminare "requisiti di configurazione".
2. Seguire le istruzioni riportate in "Guida all'installazione dello switch NVIDIA".

Quali sono le prossime novità?

Dopo aver installato l'hardware, puoi"rivedere il cablaggio e la configurazione" requisiti.

Esaminare le considerazioni relative al cablaggio e alla configurazione

Prima di configurare lo switch NVIDIA SN2100, fare riferimento alle seguenti considerazioni.

Dettagli della porta NVIDIA

Porte switch	Utilizzo delle porte
swp1s0-3	4 nodi di porte cluster breakout da 10 GbE
swp2s0-3	4 nodi di porte cluster breakout da 25 GbE
swp3-14	Nodi di porta cluster 40/100GbE
swp15-16	100GbE porte Inter-Switch link (ISL)

Vedere "Hardware Universe" per ulteriori 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` eseguire il 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 di rame da 40 GbE/100 GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Aggiungere le due righe seguenti a `/etc/cumulus/switchd.conf` File per ogni porta (swpg <n>) che utilizza cavi in rame da 40 GbE/100 GbE:

   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   Ad 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 `switchd` servizio:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Verificare che le porte siano in funzione:

```
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 di rame da 40 GbE/100 GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface --view=pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Configurare i collegamenti utilizzando `nv set` eseguire il comando come segue:
   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Ricaricare `switchd` servizio

   Ad 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 in funzione:

```
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)
```

Per "Lo switch SN2100 non riesce a collegarsi utilizzando cavi in rame 40/100GbE" ulteriori informazioni, consultare l'articolo della Knowledge base.

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. Ad esempio:

- AFF A800 sulle porte e0a e e0b
- AFF A320 sulle porte e0g e e0h

Adattatore QSA

Quando si utilizza un adattatore QSA per connettersi alle porte del cluster 10GbE/25GbE su una piattaforma, il collegamento potrebbe non essere disponibile.

Per risolvere il problema, procedere come segue:

- Per 10GbE, impostare manualmente la velocità di collegamento swp1s0-3 su 10000 e impostare la negoziazione automatica su Off.
- Per 25GbE, impostare manualmente la velocità di collegamento swp2s0-3 su 25000 e impostare la negoziazione automatica su Off.

> Quando si utilizzano adattatori QSA 10GbE/25GbE, inserirli nelle porte 40GbE/100GbE senza interruzione (swp3-swp14). Non inserire l'adattatore QSA in una porta configurata per il breakout.

Impostazione della velocità dell'interfaccia sulle porte di breakout

A seconda del ricetrasmettitore nella porta dello switch, potrebbe essere necessario impostare la velocità sull'interfaccia dello switch su una velocità fissa. Se si utilizzano porte breakout 10GbE e 25GbE, verificare che la negoziazione automatica sia disattivata e impostare la velocità dell'interfaccia sullo switch.

Cumulus Linux 4.4.3

Ad 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 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

Ad 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
off
  duplex                full                  full
full
  speed                 10G                   10G
10G
  fec                   auto                  auto
auto
  mtu                   9216                  9216
9216
[breakout]

  state                 up                    up
up
```

Controllare lo stato dell'interfaccia e della porta per verificare che le impostazioni siano 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)
.
.
```

Quali sono le prossime novità?

Dopo aver esaminato i requisiti di cablaggio e configurazione, è possibile"cablare i ripiani NS224 come spazio di archiviazione collegato all'interruttore" .

Cablare gli shelf NS224 come storage collegato allo switch

Se si dispone di un sistema in cui gli shelf di dischi NS224 devono essere cablati come storage collegato allo switch (non come storage collegato direttamente), utilizzare le informazioni fornite qui.

- Cablare gli shelf di dischi NS224 attraverso gli switch di storage:

  "Cablaggio degli shelf di dischi NS224 collegati allo switch"

- Verificare l'hardware supportato, ad esempio switch e cavi storage, per il modello di piattaforma in uso:

  "NetApp Hardware Universe"

Quali sono le prossime novità?

Dopo aver cablato i tuoi scaffali, puoi"configurare lo switch" .

Configurare il software

Workflow di installazione del software per switch NVIDIA SN2100

Per installare e configurare il software per uno switch NVIDIA SN2100, attenersi alla seguente procedura:

1. **"Configurare lo switch"**

   Configurare lo switch NVIDIA SN2100.

2. **"Installare Cumulus Linux in modalità Cumulus"**

   È possibile installare il sistema operativo Cumulus Linux (CL) quando lo switch esegue Cumulus Linux.

3. **"Installare 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. **"Installare o aggiornare lo script RCF (Reference Configuration file)"**

   Sono disponibili due script RCF per le applicazioni di clustering e storage. La procedura per ciascuno di essi è la stessa.

6. **"Installare il file CSHM"**

   È possibile installare il file di configurazione applicabile per il monitoraggio dello stato degli switch Ethernet degli switch cluster NVIDIA.

7. **"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, consultare la documentazione di NVIDIA.

Fasi

1. Esaminare "requisiti di configurazione".
2. Seguire le istruzioni riportate in "Sistema NVIDIA Bring-Up.".

Quali sono le prossime novità?

Dopo aver configurato lo switch, puoi"installare Cumulus Linux in modalità Cumulus" O"installare Cumulus Linux in modalità ONIE" .

Installare 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 "Installare in modalità ONIE").

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Conoscenza di livello intermedio di Linux.
- Familiarità con la modifica di base del testo, le autorizzazioni dei file UNIX e il monitoraggio dei processi. Sono preinstallati diversi editor di testo, tra cui `vi` e. `nano`.
- Accesso a una shell Linux o UNIX. Se si utilizza Windows, utilizzare un ambiente Linux come strumento della riga di comando per interagire con Cumulus Linux.
- Il requisito della velocità di trasmissione 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

A proposito di questa attività

Tenere presente 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 si accede a Cumulus Linux, è necessario modificare questa password predefinita. Assicurarsi di aggiornare gli script di automazione prima di installare una nuova immagine. Cumulus Linux offre opzioni della riga di comando per modificare automaticamente la password predefinita durante il processo di installazione.

Esempio 1. Fasi

Cumulus Linux 4.4.3

1. Accedere allo switch.

   La prima volta che si accede allo switch, è necessario specificare il nome utente/la 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. Controllare 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 il riavvio della sessione console/SSH.

   > Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificamente per l'utilizzo della gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.

Non utilizzare caratteri di sottolineatura (_), apostrofo (') o 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 `/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 la data, l'ora, il fuso orario e il server NTP sullo switch.
   a. Verificare il fuso orario corrente:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Aggiornamento al nuovo fuso orario:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Verificare il fuso orario corrente:

```
cumulus@switch:~$ date +%Z
```

d. Per impostare il fuso orario mediante la procedura guidata, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Impostare l'orologio del software in base al fuso orario configurato:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Impostare il valore corrente dell'orologio del software sull'orologio hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Se necessario, aggiungere un server NTP:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Verificare che `ntpd` sia 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 di origine NTP. Per impostazione predefinita, l'interfaccia di origine utilizzata da NTP è `eth0`. È possibile configurare una diversa interfaccia di origine NTP nel modo seguente:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Installare 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. Digitare **y** quando richiesto.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione viene avviata automaticamente e vengono visualizzate le seguenti opzioni della schermata di GRUB. Non effettuare alcuna selezione.
   - Cumulus-Linux GNU/Linux
   - ONIE: Installare il sistema operativo
   - INSTALLAZIONE DI CUMULUS
   - Cumulus-Linux GNU/Linux
9. Ripetere i passaggi da 1 a 4 per accedere.
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. Creare un nuovo utente e aggiungerlo 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. Accedere allo switch.

   La prima volta che si accede allo switch, è necessario specificare il nome utente/la 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. Controllare 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 il riavvio della sessione console/SSH.

> Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificamente per l'utilizzo della gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.

> Non utilizzare caratteri di sottolineatura (_), apostrofo (') o 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 `/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. Per impostare il fuso orario:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verificare il fuso orario corrente:

```
cumulus@switch:~$ date +%Z
```

   c. Per impostare il fuso orario mediante la procedura guidata, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

   d. Impostare l'orologio del software in base al fuso orario configurato:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Impostare il valore corrente dell'orologio del software sull'orologio hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Se necessario, aggiungere un server NTP:

```
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` sia 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 di origine NTP. Per impostazione predefinita, l'interfaccia di origine utilizzata da NTP è `eth0`. È possibile configurare una diversa interfaccia di origine NTP nel modo seguente:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installare 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. Digitare **y** quando richiesto.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione viene avviata automaticamente e vengono visualizzate le seguenti opzioni della schermata di GRUB. Non effettuare alcuna selezione.
   - Cumulus-Linux GNU/Linux
   - ONIE: Installare il sistema operativo
   - INSTALLAZIONE DI CUMULUS
   - Cumulus-Linux GNU/Linux
9. Ripetere i passaggi da 1 a 4 per accedere.

10. Verificare che la versione di Cumulus Linux sia la 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 i nodi dispongano di una connessione a ciascuno 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. Creare un nuovo utente e aggiungerlo 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 ulteriori gruppi di utenti 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 "NVIDIA User account (account utente NVIDIA)" per ulteriori informazioni.

Cumulus Linux 5.11.0

1. Accedere allo switch.

   Quando si accede allo switch per la prima volta, richiede il nome utente/password di **cumulus** /**cumulus** con `sudo` Privileges.

```
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. Controllare 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 il riavvio della sessione console/SSH.

   Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificamente per l'utilizzo della gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.

   Non utilizzare caratteri di sottolineatura (_), apostrofo (') o 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 `/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. Per impostare il fuso orario:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verificare il fuso orario corrente:

```
cumulus@switch:~$ date +%Z
```

   c. Per impostare il fuso orario mediante la procedura guidata, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Impostare l'orologio del software in base al fuso orario configurato:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Impostare il valore corrente dell'orologio del software sull'orologio hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Se necessario, aggiungere un server NTP:

```
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` sia 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 di origine NTP. Per impostazione predefinita, l'interfaccia di origine utilizzata da NTP è `eth0`. È possibile configurare una diversa interfaccia di origine NTP nel modo seguente:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installare 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. Digitare **y** quando richiesto.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione viene avviata automaticamente e vengono visualizzate le seguenti opzioni della schermata di GRUB. Non effettuare alcuna selezione.
   - Cumulus-Linux GNU/Linux
   - ONIE: Installare il sistema operativo
   - INSTALLAZIONE DI CUMULUS
   - Cumulus-Linux GNU/Linux
9. Ripetere i passaggi da 1 a 4 per accedere.
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 disponga di una connessione a ciascuno 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
```

Per ulteriori informazioni, vedere "NVIDIA User account (account utente NVIDIA)" .

Quali sono le prossime novità?

Dopo aver installato Cumulus Linux in modalità Cumulus, "installare lo script del file di configurazione di riferimento (RCF)".

Installare 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 "Installare in modalità Cumulus").

A proposito di questa attività

È possibile installare Cumulus Linux utilizzando Open Network Install Environment (ONIE) che consente il rilevamento automatico di un'immagine del programma di installazione di rete. Questo semplifica il modello di sistema per la protezione degli switch con una scelta di sistemi operativi, come Cumulus Linux. Il modo più semplice per installare Cumulus Linux con ONIE consiste nel rilevamento HTTP locale.

Se l'host è abilitato per IPv6, assicurarsi che sia in esecuzione un server Web. Se l'host è abilitato per IPv4, assicurarsi che sia in esecuzione DHCP oltre a un server Web.

Questa procedura illustra come aggiornare Cumulus Linux dopo l'avvio dell'amministratore in ONIE.

Esempio 2. Fasi

Cumulus Linux 4.4.3

1. Scaricare il file di installazione di Cumulus Linux nella directory principale del server Web. Rinominare il file in: `onie-installer`.
2. Collegare l'host alla porta Ethernet di gestione dello switch utilizzando un cavo Ethernet.
3. Accendere lo switch.

   Lo switch scarica il programma di installazione dell'immagine ONIE e si avvia. Al termine dell'installazione, nella finestra del terminale viene visualizzato il prompt di accesso di 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 di GNU GRUB per interrompere il normale processo di avvio, selezionare **ONIE** e premere **Invio**.
6. Nella schermata successiva, selezionare **ONIE: Install OS**.
7. Il processo di ricerca del programma di installazione di ONIE esegue la ricerca dell'installazione automatica. Premere **Invio** per interrompere temporaneamente il processo.
8. Quando il processo di rilevamento si è arrestato:

   ```
   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 viene 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 inserite correttamente.
12. Installare 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, accedere 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. Rinominare il file in: `onie-installer`.
2. Collegare l'host alla porta Ethernet di gestione dello switch utilizzando un cavo Ethernet.
3. Accendere lo switch.

   Lo switch scarica il programma di installazione dell'immagine ONIE e si avvia. Al termine dell'installazione, nella finestra del terminale viene visualizzato il prompt di accesso di 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 di 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
|
|
|
|
|
|
|
|
|
|
|
+-------------------------------------------------------------------------
------+
```

Selezionare ONIE: **Install OS.**

6. Il processo di ricerca del programma di installazione di ONIE esegue la ricerca dell'installazione automatica. Premere **Invio** per interrompere temporaneamente il processo.
7. Quando il processo di rilevamento si è arrestato:

```
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. Installare 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, accedere 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. Creare un nuovo utente e aggiungerlo 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 ulteriori gruppi di utenti 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 "NVIDIA User account (account utente NVIDIA)" per ulteriori informazioni.

Quali sono le prossime novità?

Dopo aver installato Cumulus Linux in modalità ONIE, puoi"installare lo script del file di configurazione di riferimento (RCF)" .

Aggiornare le versioni di Cumulus Linux

Completare la seguente procedura per aggiornare la versione di Cumulus Linux secondo necessità.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Conoscenza di livello intermedio di Linux.
- Familiarità con la modifica di base del testo, le autorizzazioni dei file UNIX e il monitoraggio dei processi. Sono preinstallati diversi editor di testo, tra cui `vi` e. `nano`.
- Accesso a una shell Linux o UNIX. Se si utilizza Windows, utilizzare un ambiente Linux come strumento della riga di comando per interagire con Cumulus Linux.
- Il requisito della velocità di trasmissione 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

A proposito di questa attività

Tenere presente quanto segue:

> Ogni volta che Cumulus Linux viene aggiornato, l'intera struttura del file system viene cancellata e ricostruita. La configurazione esistente verrà cancellata. È necessario salvare e registrare la configurazione dello switch prima di aggiornare Cumulus Linux.

La password predefinita per l'account utente cumulus è **cumulus**. La prima volta che si accede a Cumulus Linux, è necessario modificare questa password predefinita. È necessario aggiornare gli script di automazione prima di installare una nuova immagine. Cumulus Linux offre opzioni della riga di comando per modificare automaticamente la password predefinita durante il processo di installazione.

Per ulteriori informazioni, vedere "Installazione di una nuova immagine Cumulus Linux".

Esempio 3. Fasi

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

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

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

6. Controllare la versione corrente di Cumulus Linux e le porte collegate:

```
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 di 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. Modificare 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. Controllare 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. Modificare 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/synced/synced.conf
.
.
```

12. Disconnettersi e accedere nuovamente allo switch per visualizzare il nome aggiornato dello switch 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. Impostare 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. Creare un nuovo utente e aggiungerlo 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 ulteriori gruppi di utenti 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 "NVIDIA User account (account utente NVIDIA)" per ulteriori 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. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster:

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

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

6. Controllare la versione corrente di Cumulus Linux e le porte collegate:

```
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 di 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. Modificare 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. Controllare 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. Modificare 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/synced/synced.conf
.
.
```

12. Disconnettersi e accedere nuovamente allo switch per visualizzare il nome aggiornato dello switch 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. Impostare 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. Creare un nuovo utente e aggiungerlo 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 ulteriori gruppi di utenti 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 "NVIDIA User account (account utente NVIDIA)" per ulteriori 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. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster:

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

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

6. Controllare la versione corrente di Cumulus Linux e le porte collegate:

```
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 di 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. Modificare 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. Controllare 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. Modificare 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/synced/synced.conf
.
.
```

12. Disconnettersi e riconnettersi 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 5.11.0-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. Impostare 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
```

Quali sono le prossime novità?

Dopo aver aggiornato la versione di Cumulus Linux, puoi"installare o aggiornare lo script RCF" .

Installare o aggiornare lo script RCF (Reference Configuration file)

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 le seguenti opzioni:

- Cumulus Linux è installato. Vedere "Hardware Universe" per le versioni supportate.
- Indirizzo IP, subnet mask e gateway predefinito definiti tramite DHCP o configurati manualmente.

È necessario specificare un utente nell'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:

Cluster	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.
Storage	Tutte le porte sono configurate per connessioni di archiviazione NVMe da 100 GbE.

Versioni correnti degli script RCF

Sono disponibili due script RCF per le applicazioni cluster e storage. Scaricare gli RCF dalla "Download del software NVIDIA SN2100" pagina. La procedura per ciascuno di essi è la stessa.

- Cluster: **MSN2100-RCF-v1.*x*-Cluster-ha-Breakout-LLDP**
- Storage: **MSN2100-RCF-v1.*x*-Storage**

A proposito degli esempi

La seguente procedura di esempio mostra come scaricare e applicare lo script RCF per gli switch del cluster.

L'output di 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. Fasi

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

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

   ```
   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. Visualizzare 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 python RCF 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 le istruzioni elencate nell'esempio precedente.

> Nel passaggio 3 **aggiornamento del file MOTD** precedente, il comando `cat /etc/motd` è eseguito. Questo consente di verificare il nome file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.

> Per qualsiasi problema di script RCF python che non può essere corretto, contatta "Supporto NetApp" per assistenza.

4. Riapplicare le eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a "Esaminare le considerazioni relative al cablaggio e alla configurazione" per i dettagli su eventuali ulteriori modifiche necessarie.
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 relative al ricetrasmettitore 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 i nodi dispongano di una connessione a ciascuno 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 funzionanti in 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 dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono presenti 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 funzioni correttamente:

   ```
   cluster show
   ```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.
11. Abilitare il ripristino automatico sulle 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. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster:

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

   ```
   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. Visualizzare 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 python RCF 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 le istruzioni elencate nell'esempio precedente.

> Nel passaggio 3 **Aggiornamento del file MOTD** sopra, il comando `cat /etc/issue.net` è in esecuzione. Questo consente di verificare il nome file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.

Ad 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 di script RCF python che non può essere corretto, contatta "Supporto NetApp" per assistenza.

4. Riapplicare le eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a "Esaminare le considerazioni relative al cablaggio e alla configurazione" per i dettagli su eventuali ulteriori modifiche necessarie.
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: fd20:8b1e: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

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 in modo sicuro.

6. Verificare le informazioni relative al ricetrasmettitore 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 i nodi dispongano di una connessione a ciascuno 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 funzionanti in 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 dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono presenti 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 funzioni correttamente:

   ```
   cluster show
   ```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.
11. Abilitare il ripristino automatico sulle 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. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster:

   ```
   network device-discovery show
   ```

4. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti:

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

   b. Verificare che tutte le interfacce del 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. Disattiva l'autorevert sulle LIF del cluster. Le LIF del cluster eseguono il failover sullo switch del cluster partner e rimangono nella pagina man mano che si esegue la procedura di upgrade sullo switch target:

   ```
   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. Visualizzare 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 python RCF 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 le istruzioni elencate nell'esempio precedente.

> Nel passaggio 3 **Aggiornamento del file MOTD** sopra riportato, viene eseguito il comando `cat /etc/issue.net. Questo consente di verificare il nome file RCF, la versione RCF, le porte da utilizzare e altre informazioni importanti nel banner RCF.

Ad 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 di script RCF python che non può essere corretto, contatta "Supporto NetApp" per assistenza.

4. Riapplicare le eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a "Esaminare le considerazioni relative al cablaggio e alla configurazione" per i dettagli su eventuali ulteriori modifiche necessarie.
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: fd20:8b1e: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

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 in modo sicuro.

6. Verificare le informazioni relative al ricetrasmettitore 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 i nodi dispongano di una connessione a ciascuno 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 funzionanti in 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 dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono presenti 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 funzioni correttamente:

   ```
   cluster show
   ```

10. Ripetere i passaggi da 1 a 14 sul secondo interruttore.
11. Abilitare il ripristino automatico sulle LIF del cluster.

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

Quali sono le prossime novità?

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 **OTHER** è visualizzato per il tuo modello. Per identificare il modello del tuo switch NVIDIA, trova il codice prodotto 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 log funzionino correttamente quando si utilizza NVIDIA CL 5.11.x con le seguenti release di ONTAP. Sebbene il monitoraggio dello stato e la raccolta dei log possano comunque funzionare anche senza questi passaggi, seguirli garantisce il corretto funzionamento di tutto.
>
> - 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 in esecuzione.
- Abilitare SSH sullo switch per utilizzare tutte le funzionalità disponibili in CSHM.
- Cancellare la `/mroot/etc/cshm_nod/nod_sign/` directory su tutti i nodi:

  a. Immettere la notoresella:

     ```
     system node run -node <name>
     ```

  b. Modifica dei privilegi avanzati:

     ```
     priv set advanced
     ```

  c. Elencare i file di configurazione nella `/etc/cshm_nod/nod_sign` directory. Se la directory esiste e contiene file di configurazione, elenca i nomi dei file.

     ```
     ls /etc/cshm_nod/nod_sign
     ```

  d. Eliminare tutti i file di configurazione corrispondenti ai modelli di switch collegati.

     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 gli stessi modelli.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

  a. Verificare che i file di configurazione eliminati non siano più nella directory:

```
ls /etc/cshm_nod/nod_sign
```

Fasi

1. Scaricare il file zip di configurazione dello switch Ethernet Health monitor in base alla versione di ONTAP corrispondente. Questo file è disponibile nella "Switch Ethernet NVIDIA" pagina .
   a. Nella pagina di download del software NVIDIA SN2100, selezionare **Nvidia CSHM file**.
   b. Nella pagina attenzione/da leggere, selezionare la casella di controllo per accettare.
   c. Nella pagina Contratto di licenza con l'utente finale, selezionare la casella di controllo Accetto e fare clic su **Accetta e continua**.
   d. Nella pagina file Nvidia CSHM - Download, selezionare il file di configurazione appropriato. 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 da 9.11.1 a 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. caricare il file zip applicabile sul server Web interno.
2. Accedi alle impostazioni della modalità avanzata da uno dei sistemi ONTAP nel cluster.

   ```
   set -privilege advanced
   ```

3. Eseguire il comando di configurazione dello switch Health monitor.

   ```
   cluster1::> system switch ethernet configure-health-monitor
   ```

4. Verificare che l'output del comando termini con il seguente testo per la versione di ONTAP in uso:

ONTAP 9.15.1 e versioni successive

Il monitoraggio dello stato dello switch Ethernet ha installato il file di configurazione.

ONTAP da 9.11.1 a 9.14.1

SHM ha installato il file di configurazione.

ONTAP 9.10.1

Pacchetto scaricato CSHM elaborato correttamente.

In caso di errore, contattare il supporto NetApp.

1. attendere fino a due volte l'intervallo di polling del monitor dello stato 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 mostra ancora **ALTRO** dopo aver applicato il file di configurazione, contattare il supporto NetApp.

Vedi il "switch di sistema ethernet configura-monitor-stato" comando per ulteriori dettagli.

Quali sono le prossime novità?

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.

A proposito di questa attività

- È necessario essere collegati allo switch mediante 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"Workflow di installazione del software per switch NVIDIA SN2100" .

Esempio 5. Fasi

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`

   Ad 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

Migrare gli switch del cluster CN1610 agli switch del cluster NVIDIA SN2100

È possibile migrare gli switch cluster CN1610 di NetApp per un cluster ONTAP agli switch cluster NVIDIA SN2100. Si tratta di una procedura senza interruzioni.

Verifica dei requisiti

Quando si sostituiscono gli switch del cluster NetApp CN1610 con gli switch del cluster NVIDIA SN2100, è necessario conoscere alcune informazioni di configurazione, le connessioni delle porte e i requisiti di cablaggio. Vedere "Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100".

Switch supportati

Sono supportati i seguenti switch del cluster:

- NetApp CN1610
- NVIDIA SN2100

Per informazioni dettagliate sulle porte supportate e sulle relative configurazioni, consultare "Hardware Universe".

Prima di iniziare

Verificare che la configurazione soddisfi i seguenti requisiti:

- Il cluster esistente è configurato e funziona correttamente.
- Tutte le porte del cluster sono nello stato **up** per garantire operazioni senza interruzioni.
- Gli switch del 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 switch CN1610.
  - Connettività di gestione e accesso alla console sia per gli switch CN1610 che per i nuovi switch.
  - Tutte le LIF del cluster in stato up con le LIF del cluster sulle 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 40 GbE o 100 GbE.
- Hai pianificato, migrato e documentato la connettività da 40 GbE e 100 GbE dai nodi agli switch cluster NVIDIA SN2100.

Migrare gli switch

A proposito degli esempi

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

- Gli switch del 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* rispettivamente sul nodo 2.

- Il `cluster1::*>` 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[port]s[breakout port 0-3]. Ad esempio, quattro porte di breakout su swp1 sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

A proposito di questa attività

Questa procedura riguarda il seguente scenario:

- L'interruttore C2 viene sostituito per primo dall'interruttore SW2.
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - 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 ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - Il cablaggio tra i nodi e C1 viene quindi scollegato da C1 e ricollegato a SW1.

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

Fase 1: Preparazione per la migrazione

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

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

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

3. Disattivare il ripristino automatico sulle LIF del cluster:

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

Fase 2: Configurare le porte e il cablaggio

1. Determinare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.

   Ogni porta deve essere visualizzata per `Link` e. `healthy` per `Health Status`.

   a. Visualizzare 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
```

b. Visualizzare le informazioni relative ai LIF e ai relativi nodi principali designati:

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

Viene visualizzato ciascun LIF `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 sono collegate agli switch del cluster esistenti nel seguente modo (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 sono collegati nel seguente modo (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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124     H          AFF-A400
e3a
node2                 0/2           124     H          AFF-A400
e3a
c2                    0/13          179     S I s      CN1610
0/13
c2                    0/14          175     S I s      CN1610
0/14
c2                    0/15          179     S I s      CN1610
0/15
c2                    0/16          175     S I s      CN1610
0/16

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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124    H           AFF-A400
e3b
node2                 0/2           124    H           AFF-A400
e3b
c1                    0/13          175    S I s       CN1610
0/13
c1                    0/14          175    S I s       CN1610
0/14
c1                    0/15          175    S I s       CN1610
0/15
c1                    0/16          175    S I s       CN1610
0/16
```

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 collegate alle porte del cluster dei nodi per eseguire il failover delle 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 il cablaggio appropriato supportato da NVIDIA SN2100.
3. Visualizzare 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 seguente modo, dal punto di vista dei nodi:

   `network device-discovery show -protocol`

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)   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 di nodi siano in funzione:

   `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 delle 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 il cablaggio appropriato supportato da NVIDIA SN2100.
8. Verificare la configurazione finale del cluster:

   `network port show -ipspace Cluster`

   Ogni porta dovrebbe essere visualizzata `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 seguente modo, dal punto di vista dei nodi:

   `network device-discovery show -protocol`

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           -
```

10. Sugli switch sw1 e sw2, verificare che tutte le porte del cluster di nodi siano in funzione:

```
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 dispongano di una connessione a ciascuno 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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster:

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

2. Verificare che tutte le LIF della rete del cluster siano nuovamente presenti sulle porte domestiche:

   ```
   network interface show
   ```

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
```

3. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

4. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver migrato gli switch, puoi "configurare il monitoraggio dello stato dello switch".

Migrare da uno switch cluster Cisco a uno switch cluster NVIDIA SN2100

È possibile migrare gli switch cluster Cisco per un cluster ONTAP agli switch cluster NVIDIA SN2100. Si tratta di una procedura senza interruzioni.

Verifica dei requisiti

Quando si sostituiscono alcuni switch cluster Cisco meno recenti con switch cluster NVIDIA SN2100, è necessario conoscere alcune informazioni di configurazione, le connessioni delle porte e i 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 informazioni dettagliate sulle porte supportate e sulle relative configurazioni, consultare "Hardware Universe" .

Di cosa hai bisogno

Assicurarsi che:

- Il cluster esistente è configurato e funziona correttamente.
- Tutte le porte del cluster sono nello stato **up** per garantire operazioni senza interruzioni.
- Gli switch del 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 dispone di quanto segue:
  - Un cluster NetApp ridondante e completamente funzionale che utilizza entrambi gli switch Cisco meno recenti.
  - Connettività di gestione e accesso alla console sia agli switch Cisco meno recenti che ai nuovi switch.
  - Tutte le LIF del cluster in stato up con le LIF del cluster si trovano sulle 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 del cluster e0a e E1a nei sistemi AFF A800 o AFF C800, è possibile che vengano ricevuti pacchetti non validi dopo la conversione della velocità. Vedere "Bug 1570339" E l'articolo della Knowledge base "Errori CRC sulle porte T6 dopo la conversione da 40GbE a 100GbE" come guida.

Migrare gli switch

A proposito degli esempi

In questa procedura, vengono utilizzati gli switch del cluster Cisco Nexus 3232C, ad esempio comandi e output.

Gli esempi di 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* rispettivamente sul nodo 2.
- Il `cluster1::*>` 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[port]s[breakout port 0-3]. Ad esempio, quattro porte di breakout su swp1 sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

A proposito di questa attività

Questa procedura riguarda il seguente scenario:

- L'interruttore C2 viene sostituito per primo dall'interruttore SW2.
  - Chiudere le porte ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - 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 ai nodi del cluster. Tutte le porte devono essere chiuse contemporaneamente per evitare l'instabilità del cluster.
  - Il cablaggio tra i nodi e c1 viene quindi scollegato da c1 e ricollegato a sw1.

Fase 1: Preparazione per la migrazione

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

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

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

3. Disattivare il ripristino automatico sulle LIF del cluster:

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

Fase 2: Configurare le porte e il cablaggio

1. Determinare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.

   Ogni porta deve essere visualizzata per `Link` e sano per `Health Status`.

   a. Visualizzare 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
```

b. Visualizzare le informazioni sulle interfacce logiche e sui relativi nodi principali designati:

`network interface show -vserver Cluster`

Viene visualizzato ciascun LIF `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 di ciascun nodo sono collegate agli switch del cluster esistenti nel seguente modo (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 seguente modo (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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1         124   H           AFF-A400
e3a
node2                 Eth1/2         124   H           AFF-A400
e3a
c2                    Eth1/31        179   S I s       N3K-C3232C
Eth1/31
c2                    Eth1/32        175   S I s       N3K-C3232C
Eth1/32

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             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
c1                    Eth1/31       175    S I s       N3K-C3232C
Eth1/31
c1                    Eth1/32       175    S I s       N3K-C3232C
Eth1/32
```

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 collegate alle porte del cluster dei nodi per eseguire il failover delle 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 il cablaggio appropriato supportato da NVIDIA SN2100.
3. Visualizzare 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 seguente modo, 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 di nodi siano in funzione:

   `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 delle 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 il cablaggio appropriato supportato da NVIDIA SN2100.
8. Verificare la configurazione finale del cluster:

   `network port show -ipspace Cluster`

   Ogni porta dovrebbe essere visualizzata `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 seguente modo, 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    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 in funzione:

```
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 dispongano di una connessione a ciascuno 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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico sulle LIF del cluster:

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

2. Verificare che tutte le LIF della rete del cluster siano nuovamente presenti sulle porte domestiche:

   ```
   network interface show
   ```

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
```

3. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

4. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver migrato gli switch, puoi "configurare il monitoraggio dello stato dello switch".

Migrazione a un cluster con switch a due nodi con switch cluster NVIDIA SN2100

Se si dispone di un ambiente cluster senza switch a due nodi, è possibile migrare a un ambiente cluster con switch a due nodi utilizzando gli switch NVIDIA SN2100 per scalare oltre due nodi nel cluster.

La procedura da seguire dipende dalla presenza di due porte cluster-network 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 10GBASE-T RJ45 integrate per le porte di rete del cluster.

Verifica dei requisiti

Configurazione senza switch a due nodi

Assicurarsi che:

- La configurazione senza switch a due nodi è configurata e funziona correttamente.
- I nodi eseguono ONTAP 9.10.1P3 e versioni successive.
- Tutte le porte del cluster si trovano nello stato **up**.
- Tutte le interfacce logiche del cluster (LIFF) si trovano nello stato **up** e nelle porte home.

Configurazione dello switch cluster NVIDIA SN2100

Assicurarsi che:

- Entrambi gli switch dispongono di connettività di rete di gestione.
- Gli switch del cluster sono accessibili dalla console.
- Le connessioni switch node-to-node NVIDIA SN2100 e switch-to-switch utilizzano cavi Twinax o in fibra.

> Vedere "Esaminare le considerazioni relative al cablaggio e alla configurazione" per avvertenze e ulteriori dettagli. Il "Hardware Universe - Switch" contiene inoltre ulteriori informazioni sul cablaggio.

- I cavi ISL (Inter-Switch link) 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 utilizzano la versione più recente di Cumulus Linux
  - I file di configurazione di riferimento (RCF) vengono applicati agli switch
  - Qualsiasi personalizzazione del sito, ad esempio SMTP, SNMP e SSH, viene configurata sui nuovi switch.

    Il "Hardware Universe" contiene le informazioni più recenti sulle porte cluster effettive per le piattaforme in uso.

Migrare gli switch

A proposito degli esempi

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

- I nomi degli switch SN2100 sono *sw1* e *sw2*.
- I nomi delle SVM del cluster sono *node1* e *node2*.
- I nomi delle LIF sono rispettivamente *node1_clus1* e *node1_clus2* sul nodo 1 e *node2_clus1* e *node2_clus2* sul nodo 2.
- Il `cluster1::*>` 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[port]s[breakout port 0-3]. Ad esempio, quattro porte di breakout su swp1 sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.

Fase 1: Preparazione per la migrazione

1. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

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

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

   Il prompt avanzato (`*>`).

Fase 2: Configurare le porte e il cablaggio

Cumulus Linux 4,4.x

1. Disattivare tutte le porte rivolte ai nodi (non le porte ISL) su entrambi i nuovi switch del cluster sw1 e sw2.

   Non è necessario disattivare le porte ISL.

   I seguenti comandi disattivano 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 le porte ISL e fisiche dell'ISL tra i due switch SN2100 sw1 e sw2 siano installate 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. Disattiva tutte le porte rivolte ai nodi (non porte ISL) su entrambi i nuovi switch cluster SW1 e SW2.

   Non è necessario disattivare le porte ISL.

   I seguenti comandi disattivano 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 le porte ISL e fisiche dell'ISL tra i due switch SN2100 sw1 e sw2 siano installate sulle porte swp15 e swp16:

   ```
   nv show interface
   ```

I seguenti esempi 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     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-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     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-rcf2    Intra-Cluster Switch
ISL Port swp16  swp
```

1. verificare che tutte le porte del cluster siano attive:

   `network port show`

   Ogni porta dovrebbe essere visualizzata `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 tutte le LIF del cluster siano operative:

   `network interface show`

   Ogni LIF del cluster dovrebbe visualizzare true per `Is Home` e hanno un `Status Admin/Oper` di `up/up`.

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
```

3. Disattivare il ripristino automatico sulle 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. Scollegare il cavo dalla porta del cluster e3a sul nodo 1, quindi collegare e3a alla porta 3 sullo switch del cluster sw1, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

   Il "Hardware Universe - Switch" contiene ulteriori informazioni sul cablaggio.

5. Scollegare il cavo dalla porta del cluster e3a sul nodo 2, quindi collegare e3a alla porta 4 sullo switch del

cluster sw1, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

Cumulus Linux 4,4.x

1. sullo switch SW1, abilitare tutte le porte rivolte ai nodi.

   I seguenti comandi abilitano tutte le porte rivolte ai nodi 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 ai nodi.

   I seguenti comandi abilitano tutte le porte rivolte ai nodi 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       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-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 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/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. Visualizza informazioni sullo stato dei nodi nel cluster:

```
cluster show
```

Mostra esempio

Nell'esempio seguente vengono visualizzate informazioni sullo stato 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 del cluster e3b sul nodo 1, quindi collegare e3b alla porta 3 sullo switch del cluster sw2, utilizzando il cablaggio appropriato supportato dagli switch SN2100.
4. Scollegare il cavo dalla porta del cluster e3b sul nodo 2, quindi collegare e3b alla porta 4 sullo switch del cluster sw2, utilizzando il cablaggio appropriato supportato dagli switch SN2100.

Cumulus Linux 4,4.x

1. sullo switch SW2, abilitare tutte le porte rivolte ai nodi.

   I seguenti comandi abilitano le porte rivolte al nodo dello 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 ciascuno una connessione a ciascuno 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 ai nodi.

   I seguenti comandi abilitano le porte rivolte al nodo dello 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       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-int-rcf10
swp16
```

3. su entrambi gli switch SW1 e SW2, verificare che entrambi i nodi abbiano ciascuno una connessione a ciascuno switch:

   `nv show interface --view=lldp`

   I seguenti esempi mostrano i risultati appropriati per entrambi gli interruttori 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 informazioni sui dispositivi di rete rilevati nel 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 installate:

   `network port show -ipspace Cluster`

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono 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
```

Fase 3: Verificare la configurazione

1. Abilitare il ripristino automatico su tutte le LIF del cluster:

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

Mostra esempio

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto
-revert true

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true
```

2. Verificare che tutte le interfacce siano visualizzate `true` per `Is Home`:

   `net interface show -vserver Cluster`

   Il completamento dell'operazione potrebbe richiedere alcuni minuti.

Mostra esempio

L'esempio seguente mostra che tutte le LIF sono in su su node1 e node2 e questo `Is Home` i risultati sono veri:

```
cluster1::*> net 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
```

3. Verificare che le impostazioni siano disattivate:

   `network options switchless-cluster show`

   Mostra esempio

   L'output falso nell'esempio seguente mostra che le impostazioni di configurazione sono disattivate:

   ```
   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 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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. riportare il livello di privilegio ad admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

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 senza interruzioni (NDU).

Verifica dei requisiti

Infrastruttura di rete e cluster esistente

Assicurarsi che:

- Il cluster esistente viene verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
- Tutte le porte del cluster sono installate.
- Tutte le interfacce logiche del cluster (LIFF) sono installate sulle porte domestiche.
- ONTAP `cluster ping-cluster -node node1` Il comando indica che la connettività di base e le comunicazioni di dimensioni superiori a quelle di PMTU hanno esito positivo su tutti i percorsi.

Switch sostitutivo NVIDIA SN2100

Assicurarsi che:

- La connettività di rete di gestione sullo switch sostitutivo è funzionale.
- L'accesso della console allo switch sostitutivo è in posizione.
- Le connessioni dei nodi sono porte da swp1 a swp14.
- Tutte le porte ISL (Inter-Switch link) sono disattivate 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 completata.

Assicurarsi inoltre che eventuali personalizzazioni precedenti del sito, come STP, SNMP e SSH, vengano copiate nel nuovo switch.

È necessario eseguire il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.

Attivare la registrazione della console

NetApp consiglia vivamente di attivare la registrazione della console sui dispositivi in uso e di eseguire le seguenti operazioni quando si sostituisce lo switch:

- Lasciare attivato AutoSupport durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione del caso per tutta la durata della manutenzione. Consultare questo articolo della Knowledge base "SU92: Come eliminare la creazione automatica dei casi durante le finestre di manutenzione programmata" per ulteriori dettagli.
- Attivare la registrazione della sessione per qualsiasi sessione CLI. Per istruzioni su come attivare 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 lo switch

A proposito degli esempi

Gli esempi di 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_.
- Il prompt per le modifiche a tutti i nodi del cluster è `cluster1::*>`
- Le porte breakout hanno il formato: swp[port]s[breakout port 0-3]. Ad esempio, quattro porte di 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 del 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
--------- ------------ ---------------- ---- ---- ------------ --------
------
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


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 per la sostituzione

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

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

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

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

3. Installare l'RCF e l'immagine appropriati sullo switch, nsw2, ed eseguire le operazioni necessarie per la preparazione del 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 per gli switch del cluster dal sito *NVIDIA Support*. Seguire la procedura indicata nella pagina di download per scaricare Cumulus Linux per la versione del software ONTAP che si sta installando.

   b. L'RCF appropriato è disponibile sul sito "*Cluster NVIDIA e switch storage*" pagina. Seguire la procedura indicata nella pagina di download per scaricare l'RCF corretto per la versione del software ONTAP che si sta installando.

Fase 2: Configurare le porte e il cablaggio

Cumulus Linux 4.4.3

1. Sul nuovo switch nsw2, accedere come admin e chiudere tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da swp1 a swp14).

   Le LIF sui nodi del cluster dovrebbero essere già riuscite a eseguire 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. Disattivare il ripristino automatico sulle 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 per tutti i LIF del cluster:

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

4. Spegnere 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 dello 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 installate 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 installate 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 la porta `e3b` è attivo su tutti i nodi:

   `network port show -ipspace Cluster`

   L'output dovrebbe essere simile a quanto segue:

```
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 seguente modo, 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 di nodi siano in funzione:

   `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 dispongano di una connessione a ciascuno 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. Abilitare il ripristino automatico sulle LIF del cluster:

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

12. Sullo switch nsw2, richiamare le porte collegate alle porte di rete dei nodi.

```
cumulus@nsw2:~$ net del interface swp1-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

13. Visualizzare le informazioni sui nodi di un cluster:

```
cluster show
```

Questo esempio mostra che l'integrità del nodo per node1 e node2 in questo cluster è vera:

```
cluster1::*> cluster show

Node          Health  Eligibility
------------- ------- ------------
node1         true    true
node2         true    true
```

14. Verificare che tutte le porte del cluster fisico siano installate:

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, accedere come admin e chiudere tutte le porte che saranno connesse alle interfacce del cluster di nodi (porte da swp1 a swp14).

   Le LIF sui nodi del cluster dovrebbero essere già riuscite a eseguire 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. Disattivare il ripristino automatico sulle 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 per tutti i LIF del cluster:

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

4. Spegnere 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 dello 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 installate 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 installate 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 la porta `e3b` è attivo su tutti i nodi:

   `network port show -ipspace Cluster`

   L'output dovrebbe essere simile a quanto segue:

```
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 seguente modo, 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 di nodi siano in funzione:

   `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 dispongano di una connessione a ciascuno 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. Abilitare il ripristino automatico sulle LIF del cluster:

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

12. Sullo switch nsw2, richiamare le porte collegate alle porte di rete dei nodi.

```
cumulus@nsw2:~$ nv set interface swp1-14 link state up
cumulus@nsw2:~$ nv config apply
```

13. Visualizzare le informazioni sui nodi di un cluster:

```
cluster show
```

Questo esempio mostra che l'integrità del nodo per node1 e node2 in questo cluster è vera:

```
cluster1::*> cluster show

Node           Health  Eligibility
-------------- ------- ------------
node1          true    true
node2          true    true
```

14. Verificare che tutte le porte del cluster fisico siano installate:

```
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
```

Fase 3: Verificare la configurazione

Cumulus Linux 4.4.3

1. Verificare che la rete del cluster sia in buone condizioni.

```
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 in buone condizioni.

```
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. riportare il livello di privilegio ad admin:

```
set -privilege admin
```

2. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:

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

Quali sono le prossime novità?

Dopo aver sostituito gli interruttori, puoi "configurare il monitoraggio dello stato dello switch".

Sostituire gli switch del cluster NVIDIA SN2100 con connessioni senza switch

È possibile migrare da un cluster con una rete cluster commutata a uno in cui due nodi sono collegati direttamente per ONTAP 9.3 e versioni successive.

Verifica dei requisiti

Linee guida

Consultare le seguenti linee guida:

- La migrazione a una configurazione cluster senza switch a due nodi è un'operazione senza interruzioni. La maggior parte dei sistemi dispone di due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per i 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 funzione 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 e utilizza ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

Prima di iniziare

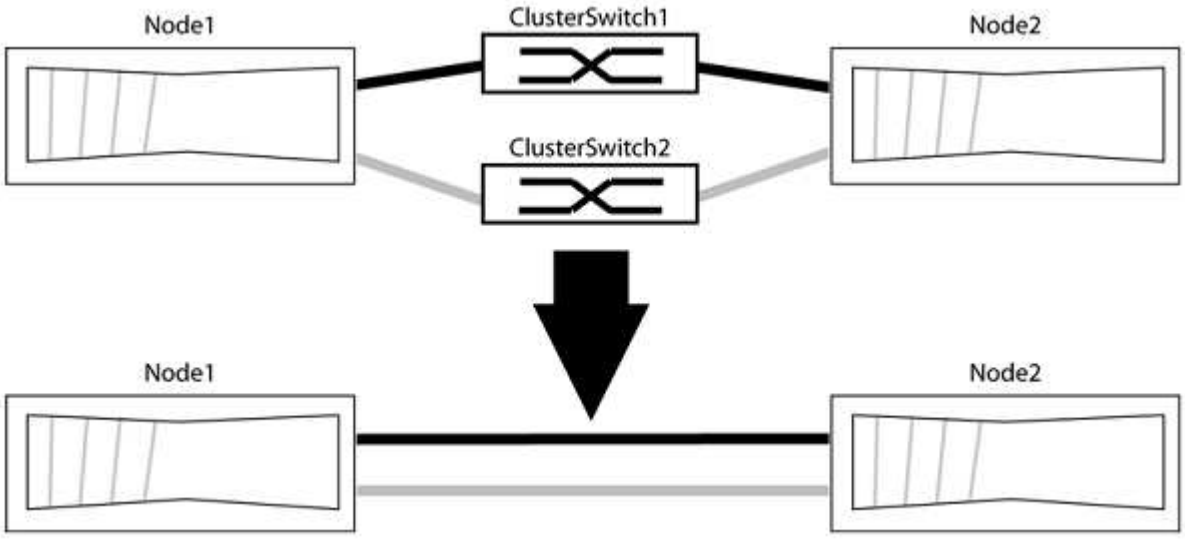
Assicurarsi di disporre di quanto segue:

- Un cluster integro costituito da due nodi collegati da switch di cluster. I nodi devono eseguire la stessa release di ONTAP.
- Ciascun nodo con il numero richiesto di porte cluster dedicate, che forniscono connessioni di interconnessione cluster ridondanti per supportare la configurazione del sistema. Ad esempio, esistono due porte ridondanti per un sistema con due porte di interconnessione cluster dedicate su ciascun nodo.

Migrare gli switch

A proposito di questa attività

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.



A proposito degli esempi

Gli esempi della seguente procedura mostrano i nodi che utilizzano "e0a" e "e0b" come porte del cluster. I nodi potrebbero utilizzare porte cluster diverse in base al sistema.

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

Il prompt avanzato `*>` viene visualizzato.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster senza switch, attivato per impostazione predefinita.

   È possibile verificare che il rilevamento dei cluster senza switch sia attivato eseguendo il comando Advanced Privilege:

   ```
   network options detect-switchless-cluster show
   ```

   Mostra esempio

   Il seguente esempio di output mostra se l'opzione è attivata.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Se "Enable Switchless Cluster Detection" (attiva rilevamento cluster senza switch) è `false`, Contattare il supporto NetApp.

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

   ```
   system node autosupport invoke -node * -type all -message
   MAINT=<number_of_hours>h
   ```

   dove `h` indica la durata della finestra di manutenzione in ore. Il messaggio informa il supporto tecnico di questa attività di manutenzione in modo che possa eliminare la creazione automatica del caso durante la finestra di manutenzione.

   Nell'esempio seguente, il comando sospende la creazione automatica del caso per due ore:

   Mostra esempio

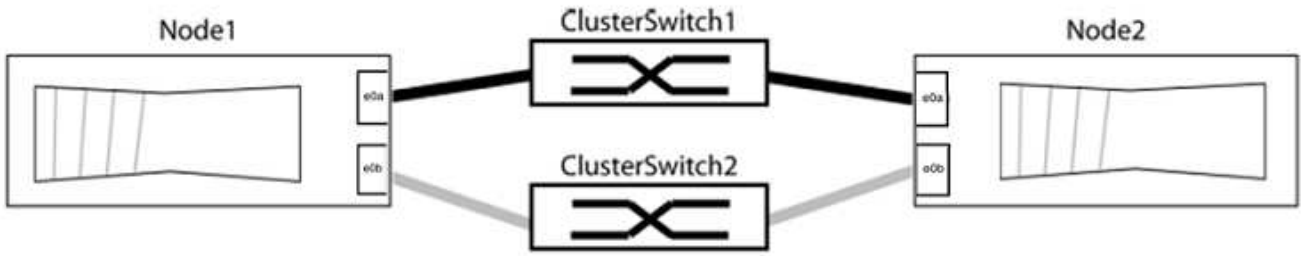
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Fase 2: Configurare le porte e il cablaggio

1. Organizzare le porte del cluster su ciascun switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano allo switch del cluster 1 e le porte del cluster nel gruppo 2 vadano allo switch2 del cluster. Questi gruppi sono richiesti più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e lo stato del collegamento:

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

Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo viene identificato come "node1:e0a" e "node2:e0a" e l'altro come "node1:e0b" e "node2:e0b". I nodi potrebbero utilizzare porte cluster diverse in quanto variano in base al sistema.



Verificare che il valore delle porte sia di `up` Per la colonna "link" e un valore di `healthy` Per la colonna "Health Status" (Stato 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 tutte le LIF del cluster si trovino sulle porte home.

   Verificare che la colonna "is-home" sia `true` Per ciascuna 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 porte home, ripristinare tali LIF alle porte home:

`network interface revert -vserver Cluster -lif *`

4. Disattivare l'autorevert per le LIF del cluster:

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

5. Verificare che tutte le porte elencate nella fase precedente siano collegate a uno switch di rete:

   `network device-discovery show -port cluster_port`

   La colonna "dispositivo rilevato" deve essere il nome dello switch del cluster a cui è collegata 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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
   ```

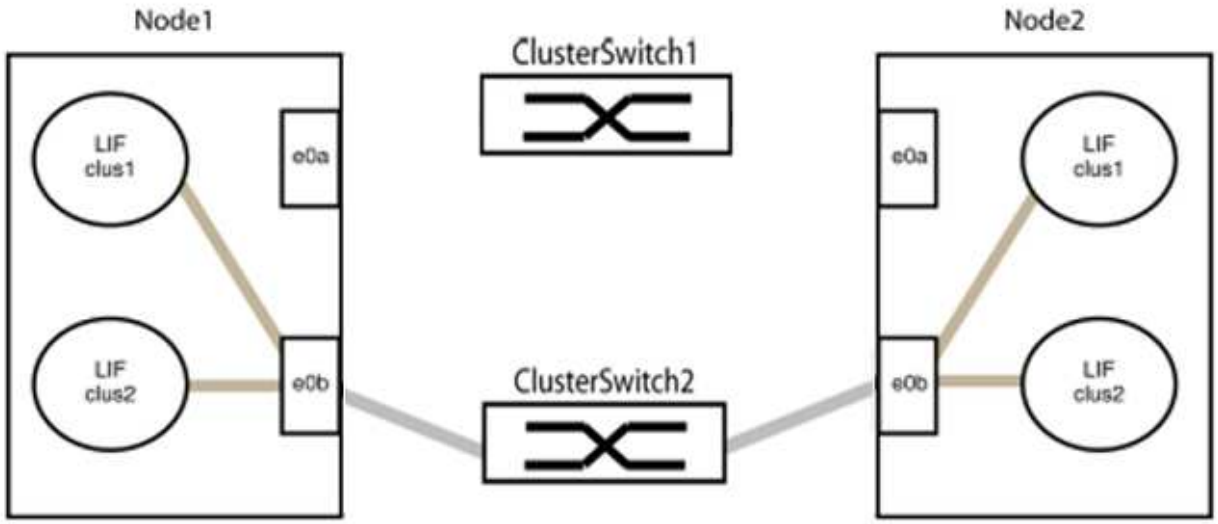
   Tutte le unità devono essere master o secondarie.

2. Impostare la configurazione senza switch per le porte del gruppo 1.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal raggruppo1 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

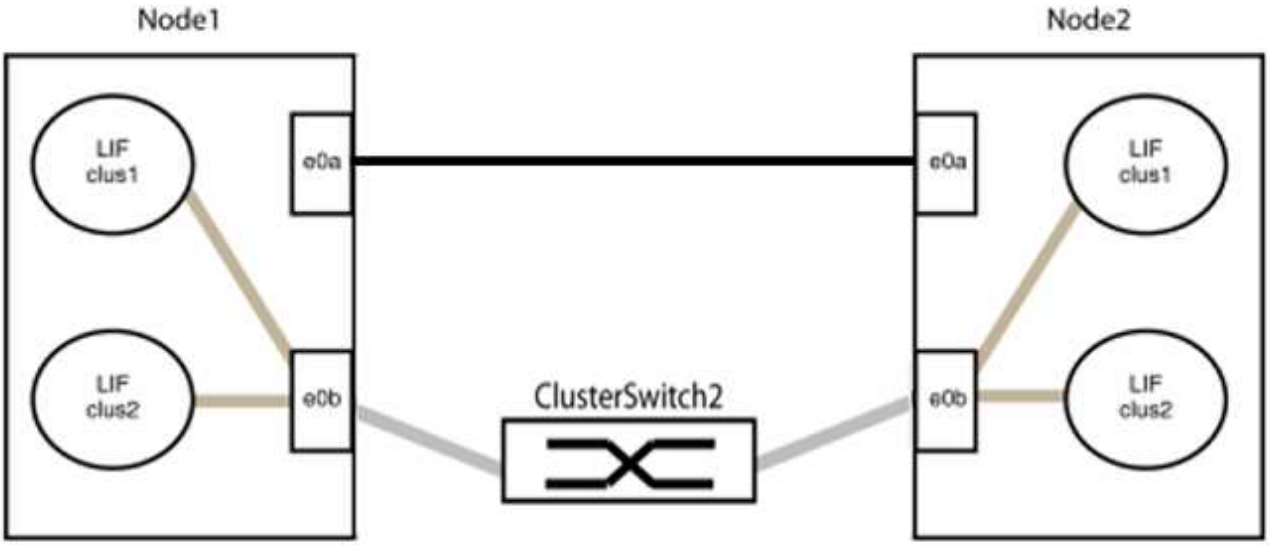
   a. Scollegare tutti i cavi dalle porte del raggruppo1 contemporaneamente.

      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 da una parte all'altro.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2:



3. L'opzione di rete del cluster senza switch passa da `false` a. `true`. Questa operazione potrebbe richiedere fino a 45 secondi. Verificare che l'opzione switchless sia impostata su `true`:

`network options switchless-cluster show`

Il seguente esempio mostra che il cluster senza switch 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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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)
```

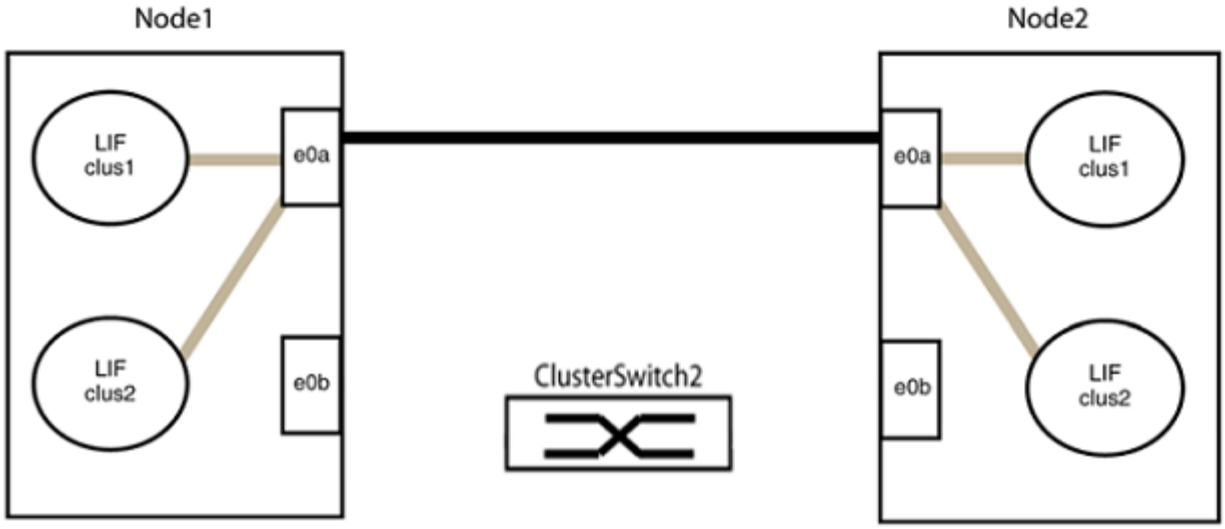
Prima di passare alla fase successiva, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

1. impostare la configurazione senza switch per le porte del gruppo 2.

   Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 2 e ricollegarle il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

   a. Scollegare tutti i cavi dalle porte del raggruppo2 contemporaneamente.

      Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0b" su ciascun nodo e il traffico del cluster continua attraverso la connessione diretta tra le porte "e0a":



b. Collegare le porte del group2 in modo che si inserano nella parte posteriore.

Nell'esempio seguente, "e0a" sul nodo 1 è collegato a "e0a" sul nodo 2 e "e0b" sul nodo 1 è collegato a "e0b" sul nodo 2:

Fase 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 collegate correttamente 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 le LIF del cluster:

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

3. Verificare che tutte le LIF siano a casa. Questa operazione potrebbe richiedere alcuni secondi.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Mostra esempio

I LIF sono stati ripristinati se la colonna "is Home" è `true`, come illustrato per `node1_clus2` e. `node2_clus2` nel seguente esempio:

```
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 dei cluster LIFS non è tornato alle porte home, ripristinarli 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 nodi:

   `cluster show`

   Mostra esempio

   L'esempio seguente mostra epsilon su entrambi i nodi da visualizzare `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

È possibile utilizzare `network interface check cluster-connectivity` per avviare un controllo di accessibilità per la connettività del cluster e 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
                                  Source           Destination
Packet
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 release di ONTAP

Per tutte le release di ONTAP, è possibile utilizzare anche `cluster ping-cluster -node <name>` comando per controllare 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 è stata soppressa la creazione automatica dei casi, riattivarla richiamando un messaggio AutoSupport:

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

   Per ulteriori informazioni, vedere "Articolo della Knowledge base di NetApp 1010449: Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificate".

2. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

Quali sono le prossime novità?

Dopo aver sostituito gli interruttori, puoi "configurare il monitoraggio dello stato dello switch".

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.