



## **Cisco Nexus 3132Q-V**

Install and maintain

NetApp

February 13, 2026

# Sommario

Cisco Nexus 3132Q-V .....	1
Iniziare .....	1
Flusso di lavoro di installazione e configurazione per gli switch Cisco Nexus 3132Q-V .....	1
Requisiti di configurazione per gli switch Cisco Nexus 3132Q-V .....	1
Requisiti di documentazione per gli switch Cisco Nexus 3132Q-V .....	2
Requisiti di Smart Call Home .....	4
Installare l'hardware .....	4
Flusso di lavoro di installazione hardware per gli switch Cisco Nexus 3132Q-V .....	4
Foglio di lavoro completo sul cablaggio Cisco Nexus 3132Q-V .....	5
Installare lo switch cluster 3132Q-V .....	8
Installare uno switch cluster Cisco Nexus 3132Q-V in un cabinet NetApp .....	9
Esaminare le considerazioni sul cablaggio e sulla configurazione .....	13
Configurare il software .....	13
Flusso di lavoro di installazione del software per gli switch cluster Cisco Nexus 3132Q-V .....	13
Configurare lo switch Cisco Nexus 3132Q-V .....	14
Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento .....	17
Installa il software NX-OS .....	23
Installare o aggiornare l'RCF .....	40
Verifica la tua configurazione SSH .....	74
Ripristinare lo switch del cluster 3132Q-V ai valori predefiniti di fabbrica .....	76
Migrare gli switch .....	76
Migrazione da cluster senza switch a cluster con switch a due nodi .....	76
Sostituire gli interruttori .....	100
Requisiti per la sostituzione degli switch cluster Cisco Nexus 3132Q-V .....	100
Sostituire gli switch cluster Cisco Nexus 3132Q-V .....	104
Sostituisci gli switch cluster Cisco Nexus 3132Q-V con connessioni switchless .....	130

# Cisco Nexus 3132Q-V

## Iniziare

### Flusso di lavoro di installazione e configurazione per gli switch Cisco Nexus 3132Q-V

Gli switch Cisco Nexus 3132Q-V possono essere utilizzati come switch cluster nel cluster AFF o FAS . Gli switch cluster consentono di creare cluster ONTAP con più di due nodi.

Segui questi passaggi del flusso di lavoro per installare e configurare lo switch Cisco Nexus 3132Q-V.

1

#### "Requisiti di configurazione"

Esaminare i requisiti di configurazione per lo switch cluster 3132Q-V.

2

#### "Documentazione richiesta"

Consultare la documentazione specifica dello switch e del controller per configurare gli switch 3132Q-V e il cluster ONTAP .

3

#### "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.

4

#### "Installare l'hardware"

Installare l'hardware dello switch.

5

#### "Configurare il software"

Configurare il software dello switch.

### Requisiti di configurazione per gli switch Cisco Nexus 3132Q-V

Per l'installazione e la manutenzione dello switch Cisco Nexus 3132Q-V, assicurarsi di rivedere i requisiti di rete e di configurazione.

#### Requisiti di configurazione

Per configurare il cluster, è necessario disporre del numero e del tipo appropriati di cavi e connettori per i propri switch. A seconda del tipo di switch che si sta configurando inizialmente, è necessario connettersi alla porta della console dello switch tramite il cavo della console incluso; è inoltre necessario fornire informazioni di rete specifiche.

## Requisiti di rete

Per tutte le configurazioni dello switch sono necessarie le seguenti informazioni di rete:

- Subnet IP per il traffico di rete di gestione.
- Nomi host e indirizzi IP per ciascuno dei controller del sistema di archiviazione e tutti gli switch applicabili.
- La maggior parte dei controller dei sistemi di storage vengono gestiti tramite l'interfaccia e0M, collegandosi alla porta di servizio Ethernet (icona a forma di chiave inglese). Nei sistemi AFF A800 e AFF A700 , l'interfaccia e0M utilizza una porta Ethernet dedicata.

Fare riferimento al "[Hardware Universe](#)" per le ultime informazioni. Vedere "[Quali informazioni aggiuntive mi servono per installare la mia attrezzatura che non è presente in HWU?](#)" per maggiori informazioni sui requisiti di installazione degli switch.

## Cosa c'è dopo?

Dopo aver esaminato i requisiti di configurazione, è possibile rivedere il "[documentazione richiesta](#)".

## Requisiti di documentazione per gli switch Cisco Nexus 3132Q-V

Per l'installazione e la manutenzione dello switch Cisco Nexus 3132Q-V, assicurarsi di consultare tutta la documentazione consigliata.

### Documentazione dello switch

Per configurare gli switch Cisco Nexus 3132Q-V, è necessaria la seguente documentazione dal "[Supporto per gli switch Cisco Nexus serie 3000](#)" pagina.

Titolo del documento	Descrizione
<i>Guida all'installazione dell'hardware della serie Nexus 3000</i>	Fornisce informazioni dettagliate sui requisiti del sito, dettagli sull'hardware dello switch e opzioni di installazione.
<i>Guide alla configurazione del software dello switch Cisco Nexus serie 3000</i> (scegli la guida per la versione NX-OS installata sugli switch)	Fornisce le informazioni di configurazione iniziale dello switch necessarie prima di poterlo configurare per il funzionamento ONTAP .
<i>Guida all'aggiornamento e al downgrade del software Cisco Nexus serie NX-OS</i> (scegli la guida per la versione NX-OS installata sui tuoi switch)	Fornisce informazioni su come effettuare il downgrade dello switch al software dello switch supportato ONTAP , se necessario.
<i>Indice principale di riferimento dei comandi NX-OS della serie Cisco Nexus 3000</i>	Fornisce collegamenti ai vari riferimenti ai comandi forniti da Cisco.

Titolo del documento	Descrizione
<i>Riferimento MIB Cisco Nexus 3000</i>	Describe i file MIB (Management Information Base) per gli switch Nexus 3000.
<i>Riferimento ai messaggi di sistema NX-OS della serie Nexus 3000</i>	Describe i messaggi di sistema per gli switch Cisco Nexus serie 3000, quelli informativi e altri che potrebbero aiutare a diagnosticare problemi con i collegamenti, l'hardware interno o il software di sistema.
<i>Note sulla versione NX-OS della serie Cisco Nexus 3000 (selezionare le note per la versione NX-OS installata sugli switch)</i>	Describe le funzionalità, i bug e le limitazioni della serie Cisco Nexus 3000.
Informazioni normative, di conformità e di sicurezza per Cisco Nexus 6000, Cisco Nexus serie 5000, Cisco Nexus serie 3000 e Cisco Nexus serie 2000	Fornisce informazioni sulla conformità alle agenzie internazionali, sulla sicurezza e sugli statuti per gli switch della serie Nexus 3000.

### Documentazione dei sistemi ONTAP

Per configurare un sistema ONTAP , sono necessari i seguenti documenti per la versione del sistema operativo da "[ONTAP 9](#)" .

Nome	Descrizione
Istruzioni di installazione e configurazione specifiche del controller	Describe come installare l'hardware NetApp .
Documentazione ONTAP	Fornisce informazioni dettagliate su tutti gli aspetti delle versioni ONTAP .
<a href="#">"Hardware Universe"</a>	Fornisce informazioni sulla configurazione hardware e sulla compatibilità NetApp .

### Documentazione del kit ferroviario e dell'armadio

Per installare uno switch Cisco 3132Q-V in un cabinet NetApp , consultare la seguente documentazione hardware.

Nome	Descrizione
<a href="#">"Armadio di sistema 42U, guida profonda"</a>	Describe le FRU associate al cabinet del sistema 42U e fornisce istruzioni per la manutenzione e la sostituzione delle FRU.
<a href="#">"Installare lo switch Cisco Nexus 3132Q-V in un cabinet NetApp"</a>	Describe come installare uno switch Cisco Nexus 3132Q-V in un cabinet NetApp a quattro montanti.

## Requisiti di Smart Call Home

Per utilizzare Smart Call Home, è necessario configurare uno switch di rete cluster per comunicare tramite e-mail con il sistema Smart Call Home. Inoltre, è possibile configurare facoltativamente lo switch di rete del cluster per sfruttare la funzionalità di supporto Smart Call Home integrata di Cisco.

Smart Call Home monitora i componenti hardware e software della tua rete. Quando si verifica una configurazione critica del sistema, viene generata una notifica tramite e-mail e viene inviato un avviso a tutti i destinatari configurati nel profilo di destinazione.

Smart Call Home monitora i componenti hardware e software della tua rete. Quando si verifica una configurazione critica del sistema, viene generata una notifica tramite e-mail e viene inviato un avviso a tutti i destinatari configurati nel profilo di destinazione.

Prima di poter utilizzare Smart Call Home, è necessario tenere presente i seguenti requisiti:

- Deve essere presente un server di posta elettronica.
- Lo switch deve disporre di connettività IP al server di posta elettronica.
- È necessario configurare il nome del contatto (contatto del server SNMP), il numero di telefono e le informazioni sull'indirizzo. Ciò è necessario per determinare l'origine dei messaggi ricevuti.
- Un ID CCO deve essere associato a un contratto di servizio Cisco SMARTnet appropriato per la tua azienda.
- Per registrare il dispositivo, è necessario che sia attivo il servizio Cisco SMARTnet.

IL ["Sito di supporto Cisco"](#) contiene informazioni sui comandi per configurare Smart Call Home.

## Installare l'hardware

### Flusso di lavoro di installazione hardware per gli switch Cisco Nexus 3132Q-V

Per installare e configurare l'hardware per uno switch cluster 3132Q-V, attenersi alla seguente procedura:

1

#### ["Completa il foglio di lavoro sul cablaggio"](#)

Il foglio di lavoro di cablaggio di esempio fornisce esempi di assegnazioni di porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che puoi utilizzare per configurare il tuo cluster.

2

#### ["Installare l'interruttore"](#)

Installare lo switch 3132Q-V.

3

#### ["Installare lo switch in un cabinet NetApp"](#)

Installare lo switch 3132Q-V e il pannello pass-through in un cabinet NetApp secondo necessità.

## "Rivedere il cablaggio e la configurazione"

Esaminare il supporto per le porte Ethernet NVIDIA .

### Foglio di lavoro completo sul cablaggio Cisco Nexus 3132Q-V

Se desideri documentare le piattaforme supportate, scarica un PDF da questa pagina e compila il foglio di lavoro sul cablaggio.

Il foglio di lavoro di cablaggio di esempio fornisce esempi di assegnazioni di porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che puoi utilizzare per configurare il tuo cluster.

Ogni switch può essere configurato come una singola porta 40GbE o 4 porte 10GbE.

#### Esempio di foglio di lavoro per il cablaggio

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

Interruttore del cluster A		Interruttore del cluster B	
Porta di commutazione	Utilizzo di nodi e porte	Porta di commutazione	Utilizzo di nodi e porte
1	Nodo 4x10G/40G	1	Nodo 4x10G/40G
2	Nodo 4x10G/40G	2	Nodo 4x10G/40G
3	Nodo 4x10G/40G	3	Nodo 4x10G/40G
4	Nodo 4x10G/40G	4	Nodo 4x10G/40G
5	Nodo 4x10G/40G	5	Nodo 4x10G/40G
6	Nodo 4x10G/40G	6	Nodo 4x10G/40G
7	Nodo 4x10G/40G	7	Nodo 4x10G/40G
8	Nodo 4x10G/40G	8	Nodo 4x10G/40G
9	Nodo 4x10G/40G	9	Nodo 4x10G/40G
10	Nodo 4x10G/40G	10	Nodo 4x10G/40G
11	Nodo 4x10G/40G	11	Nodo 4x10G/40G
12	Nodo 4x10G/40G	12	Nodo 4x10G/40G
13	Nodo 4x10G/40G	13	Nodo 4x10G/40G

Interruttore del cluster A		Interruttore del cluster B	
14	Nodo 4x10G/40G	14	Nodo 4x10G/40G
15	Nodo 4x10G/40G	15	Nodo 4x10G/40G
16	Nodo 4x10G/40G	16	Nodo 4x10G/40G
17	Nodo 4x10G/40G	17	Nodo 4x10G/40G
18	Nodo 4x10G/40G	18	Nodo 4x10G/40G
19	Nodo 40G 19	19	Nodo 40G 19
20	Nodo 40G 20	20	Nodo 40G 20
21	Nodo 40G 21	21	Nodo 40G 21
22	Nodo 40G 22	22	Nodo 40G 22
23	Nodo 40G 23	23	Nodo 40G 23
24	Nodo 40G 24	24	Nodo 40G 24
25-30	Prenotato	25-30	Prenotato
31	40G ISL per commutare la porta B 31	31	40G ISL per commutare la porta A 31
32	40G ISL per commutare la porta B 32	32	40G ISL per commutare la porta A 32

### Foglio di lavoro vuoto per il cablaggio

È possibile utilizzare il foglio di lavoro di cablaggio vuoto per documentare le piattaforme supportate come nodi in un cluster. La sezione *Connessioni cluster supportate* del "[Hardware Universe](#)" definisce le porte del cluster utilizzate dalla piattaforma.

Interruttore del cluster A		Interruttore del cluster B	
Porta di commutazione	Utilizzo del nodo/porta	Porta di commutazione	Utilizzo del nodo/porta
1		1	
2		2	
3		3	

Interruttore del cluster A		Interruttore del cluster B	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
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	
25-30	Prenotato	25-30	Prenotato

Interruttore del cluster A		Interruttore del cluster B	
31	40G ISL per commutare la porta B 31	31	40G ISL per commutare la porta A 31
32	40G ISL per commutare la porta B 32	32	40G ISL per commutare la porta A 32

#### Cosa c'è dopo?

Dopo aver completato i fogli di lavoro sul cablaggio, ["Installare l'interruttore"](#).

### Installare lo switch cluster 3132Q-V

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

#### Prima di iniziare

Assicurati di avere quanto segue:

- Accesso a un server HTTP, FTP o TFTP nel sito di installazione per scaricare le versioni NX-OS e RCF (Reference Configuration File) applicabili.
- Versione NX-OS applicabile, scaricata da ["Download del software Cisco"](#) pagina.
- Licenze applicabili, informazioni di rete e configurazione e cavi.
- Completato ["fogli di lavoro sul cablaggio"](#).
- RCF applicabili alla rete cluster NetApp e alla rete di gestione scaricabili dal sito di supporto NetApp all'indirizzo ["mysupport.netapp.com"](#). Tutti gli switch di rete cluster e di rete di gestione Cisco vengono forniti con la configurazione predefinita di fabbrica Cisco. Questi switch dispongono anche della versione corrente del software NX-OS, ma non hanno gli RCF caricati.
- ["Documentazione richiesta per switch e ONTAP"](#).

#### Passi

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

Se stai installando...	Poi...
Cisco Nexus 9336C-FX2 in un cabinet di sistema NetApp	Per istruzioni sull'installazione dello switch in un cabinet NetApp, consultare la guida <a href="#">_Installazione di uno switch cluster Cisco Nexus 3132Q-V e di un pannello pass-through in un cabinet NetApp</a> .
Apparecchiature in un rack Telco	Consultare le procedure fornite nelle guida all'installazione dell'hardware dello switch e nelle istruzioni di installazione e configurazione NetApp .

- Cablare la rete del cluster e gli switch della rete di gestione ai controller utilizzando i fogli di lavoro di cablaggio compilati.
- Accendere la rete del cluster e gli switch e i controller della rete di gestione.

#### Cosa succederà ora?

Facoltativamente, puoi ["Installare uno switch Cisco Nexus 3132Q-V in un cabinet NetApp"](#). Altrimenti puoi

"rivedere il cablaggio e la configurazione" requisiti.

## Installare uno switch cluster Cisco Nexus 3132Q-V in un cabinet NetApp

A seconda della configurazione, potrebbe essere necessario installare lo switch Cisco Nexus 3132Q-V e il pannello pass-through in un cabinet NetApp con le staffe standard incluse con lo switch.

### Prima di iniziare

- I requisiti di preparazione iniziale, il contenuto del kit e le precauzioni di sicurezza nel ["Guida all'installazione dell'hardware Cisco Nexus serie 3000"](#) . Prima di iniziare la procedura, rivedere questi documenti.
- Kit pannello passante, disponibile da NetApp (codice articolo X8784-R6). Il kit del pannello pass-through NetApp contiene il seguente hardware:
  - Un pannello cieco passante
  - Quattro viti 10-32 x .75
  - Quattro dadi a clip 10-32
- Otto viti 10-32 o 12-24 e dadi a clip per montare le staffe e le guide scorrevoli sui montanti anteriori e posteriori del mobile.
- Kit di guide standard Cisco per installare lo switch in un cabinet NetApp .



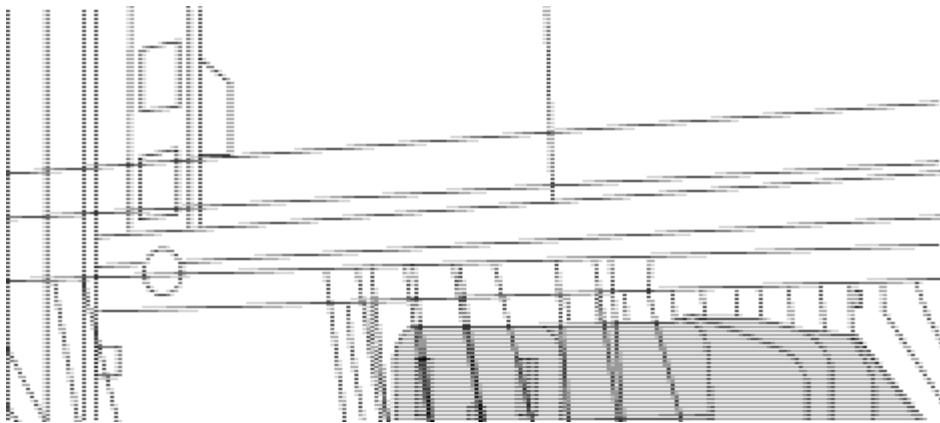
I cavi di collegamento non sono inclusi nel kit pass-through e dovrebbero essere inclusi con gli switch. Se non sono stati spediti con gli switch, è possibile ordinarli da NetApp (codice articolo X1558A-R6).

### Passi

1. Installare il pannello cieco passante nell'armadio NetApp .
  - a. Determinare la posizione verticale degli interruttori e del pannello cieco nell'armadio.

In questa procedura, il pannello cieco verrà installato in U40.

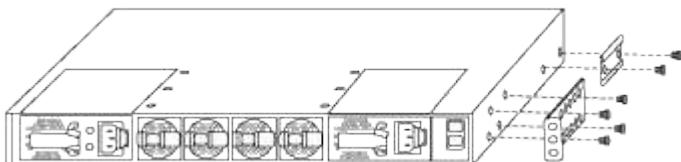
  - b. Installare due dadi a clip su ciascun lato nei fori quadrati appropriati per le guide anteriori del mobile.
  - c. Centrare il pannello verticalmente per evitare intrusioni nello spazio rack adiacente, quindi serrare le viti.
  - d. Inserire i connettori femmina di entrambi i cavi jumper da 48 pollici dalla parte posteriore del pannello e attraverso il gruppo spazzole.



(1) *Connettore femmina del cavo di collegamento.*

2. Installare le staffe di montaggio su rack sullo chassis dello switch Nexus 3132Q-V.

a. Posizionare una staffa di montaggio su rack anteriore su un lato del telaio dello switch in modo che l'aletta di montaggio sia allineata con la piastra frontale del telaio (sul lato dell'alimentatore o della ventola), quindi utilizzare quattro viti M4 per fissare la staffa al telaio.

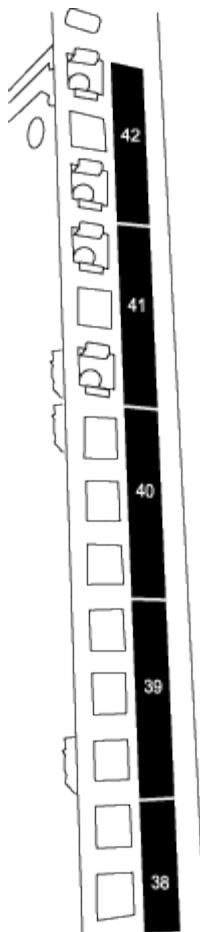


b. Ripetere il passaggio 2a con l'altra staffa di montaggio su rack anteriore sull'altro lato dello switch.

c. Installare la staffa di montaggio posteriore sul telaio dello switch.

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

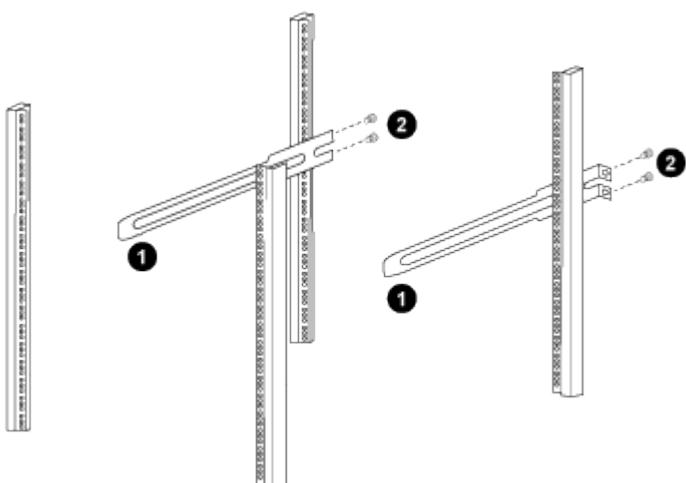
3. Installare i dadi a clip nelle posizioni dei fori quadrati per tutti e quattro i pali IEA.



I due switch 3132Q-V saranno sempre montati nella parte superiore 2U dell'armadio RU41 e 42.

4. Installare le guide scorrevoli nel mobile.

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



(1) Mentre fai scorrere delicatamente la guida scorrevole, allineala ai fori delle viti nel rack.

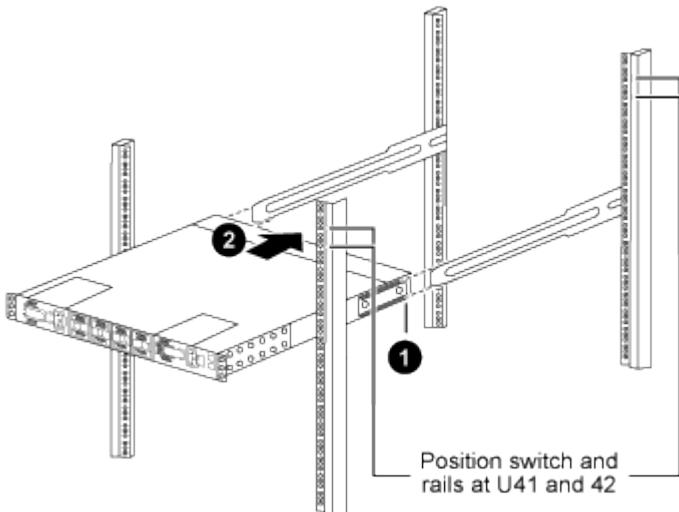
(2) Serrare le viti delle guide scorrevoli ai montanti del mobile.

- a. Ripetere il passaggio 4a per il montante posteriore destro.
  - b. Ripetere i passaggi 4a e 4b nelle posizioni RU41 sull'armadio.
5. Installare l'interruttore nell'armadio.



Per questa operazione sono necessarie due persone: una persona sostiene l'interruttore dalla parte anteriore e un'altra lo guida nelle guide scorrevoli posteriori.

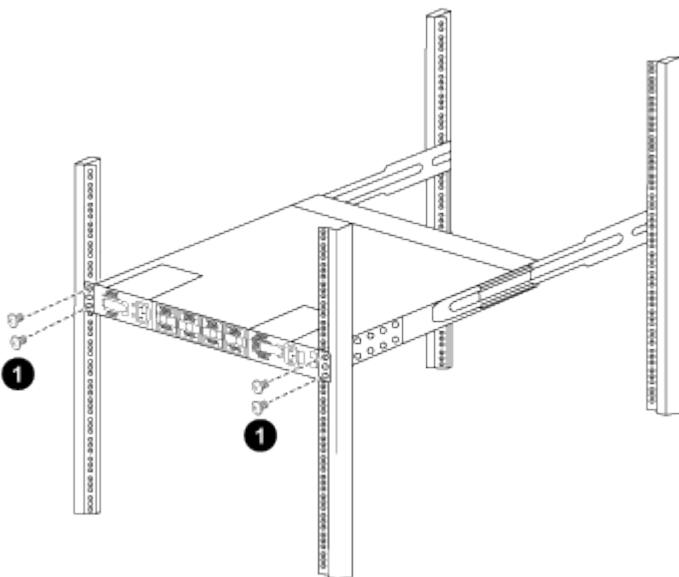
- a. Posizionare la parte posteriore dell'interruttore su RU41.



(1) *Mentre il telaio viene spinto verso i montanti posteriori, allineare le due guide di montaggio posteriori del rack con le guide scorrevoli.*

(2) *Far scorrere delicatamente l'interruttore finché le staffe di montaggio sul rack anteriore non sono a filo con i montanti anteriori.*

- b. Fissare l'interruttore all'armadietto.



(1) *Mentre una persona tiene in piano la parte anteriore del telaio, l'altra persona deve stringere completamente le quattro viti posteriori ai montanti del mobile.*

- a. Ora che il telaio è supportato senza assistenza, serrare completamente le viti anteriori ai montanti.
- b. Ripetere i passaggi da 5a a 5c per il secondo interruttore nella posizione RU42.



Utilizzando come supporto l'interruttore completamente installato, non è necessario tenere ferma la parte anteriore del secondo interruttore durante il processo di installazione.

6. Una volta installati gli interruttori, collegare i cavi di collegamento alle prese di alimentazione degli interruttori.
7. Collegare le spine maschio di entrambi i cavi di collegamento alle prese PDU più vicine disponibili.



Per mantenere la ridondanza, i due cavi devono essere collegati a PDU diverse.

8. Collegare la porta di gestione su ogni switch 3132Q-V a uno degli switch di gestione (se ordinati) oppure collegarli direttamente alla rete di gestione.

La porta di gestione è la porta in alto a destra situata sul lato PSU dello switch. Dopo l'installazione degli switch, il cavo CAT6 di ogni switch deve essere instradato attraverso il pannello passante per connettersi agli switch di gestione o alla rete di gestione.

## Esaminare le considerazioni sul cablaggio e sulla configurazione

Prima di configurare lo switch Cisco 3132Q-V, leggere le seguenti considerazioni.

### Supporto per porte Ethernet NVIDIA CX6, CX6-DX e CX7

Se si collega una porta dello switch a un controller ONTAP utilizzando le porte NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7), è necessario codificare la velocità della porta dello switch.

```
(cs1) (config) # interface Ethernet1/19
(cs1) (config-if) # speed 40000
(cs1) (config-if) # no negotiate auto
(cs1) (config-if) # exit
(cs1) (config) # exit
Save the changes:
(cs1) # copy running-config startup-config
```

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

## Configurare il software

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

Per installare e configurare il software per uno switch Cisco Nexus 3132Q-V e installare o

aggiornare il file di configurazione di riferimento (RCF), attenersi alla seguente procedura:

**1**

**"Configurare l'interruttore"**

Configurare lo switch cluster 3132Q-V.

**2**

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

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

**3**

**"Install o aggiorna il software NX-OS"**

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

**4**

**"Installare o aggiornare l'RCF"**

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

**5**

**"Verifica la configurazione SSH"**

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

**6**

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

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

## Configurare lo switch Cisco Nexus 3132Q-V

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

### Prima di iniziare

- Accesso a un server HTTP, FTP o TFTP nel sito di installazione per scaricare le versioni NX-OS e RCF (Reference Configuration File) applicabili.
- Versione NX-OS applicabile, scaricata da ["Scarica il software Cisco"](#) pagina.
- Documentazione richiesta per lo switch di rete, la documentazione del controller e la documentazione ONTAP . Per maggiori informazioni, vedere ["Documentazione richiesta"](#).
- Licenze applicabili, informazioni di rete e configurazione e cavi.
- Schede di lavoro sui cablaggi completate. Vedere ["Foglio di lavoro completo sul cablaggio Cisco Nexus 3132Q-V"](#) .
- RCF applicabili alla rete di cluster NetApp e alla rete di gestione, scaricabili dal sito di supporto NetApp all'indirizzo ["mysupport.netapp.com"](#) per gli switch che ricevi. Tutti gli switch di rete cluster e di rete di gestione Cisco vengono forniti con la configurazione predefinita di fabbrica Cisco . Questi switch dispongono anche della versione corrente del software NX-OS, ma non hanno gli RCF caricati.

### Passi

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

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

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

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

Richiesta	Risposta
Interrompere il provisioning automatico e continuare con la configurazione normale? (sì/no)	Rispondi con <b>sì</b> . L'impostazione predefinita è no.
Vuoi applicare uno standard di password sicura? (sì/no)	Rispondi con <b>sì</b> . L'impostazione predefinita è sì.
Inserisci la password per l'amministratore:	La password predefinita è "admin"; è necessario creare una nuova, più complessa. Una password debole può essere rifiutata.
Desideri accedere alla finestra di dialogo di configurazione di base? (sì/no)	Rispondere con <b>sì</b> alla configurazione iniziale dello switch.
Vuoi creare un altro account di accesso? (sì/no)	La risposta dipende dalle policy del tuo sito relative agli amministratori alternativi. L'impostazione predefinita è <b>no</b> .
Configurare la stringa di comunità SNMP di sola lettura? (sì/no)	Rispondi con <b>no</b> . L'impostazione predefinita è no.
Configurare la stringa di comunità SNMP di lettura-scrittura? (sì/no)	Rispondi con <b>no</b> . L'impostazione predefinita è no.
Inserisci il nome dello switch.	Il nome dello switch è limitato a 63 caratteri alfanumerici.

Richiesta	Risposta
Continuare con la configurazione della gestione fuori banda (mgmt0)? (sì/no)	Rispondere con <b>sì</b> (impostazione predefinita) a tale richiesta. Al prompt mgmt0 IPv4 address:, inserisci il tuo indirizzo IP: ip_address.
Configurare il gateway predefinito? (sì/no)	Rispondi con <b>sì</b> . All'indirizzo IPv4 del prompt default-gateway:, immettere default_gateway.
Configurare le opzioni IP avanzate? (sì/no)	Rispondi con <b>no</b> . L'impostazione predefinita è no.
Abilitare il servizio telnet? (sì/no)	Rispondi con <b>no</b> . L'impostazione predefinita è no.
Servizio SSH abilitato? (sì/no)	Rispondi con <b>sì</b> . L'impostazione predefinita è <b>sì</b> . <div style="display: flex; align-items: center; margin-top: 10px;"> <span data-bbox="652 739 709 802"></span> <span data-bbox="775 696 1403 844">Si consiglia di utilizzare SSH quando si utilizza Ethernet Switch Health Monitor (CSHM) per le sue funzionalità di raccolta dei log. Per una maggiore sicurezza si consiglia anche l'uso di SSHv2.</span> </div>
Inserisci il tipo di chiave SSH che vuoi generare (dsa/rsa/rsa1).	Il valore predefinito è <b>rsa</b> .
Inserire il numero di bit della chiave (1024-2048).	Inserisci i bit chiave da 1024 a 2048.
Configurare il server NTP? (sì/no)	Rispondi con <b>no</b> . L'impostazione predefinita è no.
Configurare il livello di interfaccia predefinito (L3/L2):	Rispondi con <b>L2</b> . Il valore predefinito è L2.
Configura lo stato predefinito dell'interfaccia della porta dello switch (shut/noshut):	Rispondi con <b>noshut</b> . L'impostazione predefinita è noshut.
Configurare il profilo del sistema CoPP (rigoroso/moderato/indulgente/de nso):	Rispondi con <b>rigoroso</b> . L'impostazione predefinita è rigorosa.
Vuoi modificare la configurazione? (sì/no)	A questo punto dovresti vedere la nuova configurazione. Rivedi e apporta tutte le modifiche necessarie alla configurazione appena inserita. Se sei soddisfatto della configurazione, rispondi <b>no</b> al prompt. Rispondi <b>sì</b> se desideri modificare le impostazioni di configurazione.

Richiesta	Risposta
Utilizzare questa configurazione e salvarla? (sì/no)	<p>Rispondere con <b>sì</b> per salvare la configurazione. In questo modo vengono aggiornate automaticamente le immagini di kickstart e di sistema.</p> <p> Se non si salva la configurazione in questa fase, nessuna delle modifiche sarà effettiva al successivo riavvio dello switch.</p>

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

#### Cosa succederà ora?

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

### Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento

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

#### Informazioni sugli esempi

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

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



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

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

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

#### Informazioni su questo compito

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

#### Passi

1. Se AutoSupport è abilitato su questo cluster, sopprimere la creazione automatica dei casi richiamando un

messaggio AutoSupport :

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

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



Il messaggio AutoSupport avvisa il supporto tecnico di questa attività di manutenzione, in modo che la creazione automatica dei casi venga soppressa durante la finestra di manutenzione.

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

```
set -privilege advanced
```

Il prompt avanzato(\*> ) appare.

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

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

#### Mostra esempio

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

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

-----
-----
cluster1-02/cdp
      e0a    cs1          Eth1/2      N3K-
C3132Q-V
      e0b    cs2          Eth1/2      N3K-
C3132Q-V
cluster1-01/cdp
      e0a    cs1          Eth1/1      N3K-
C3132Q-V
      e0b    cs2          Eth1/1      N3K-
C3132Q-V
```

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

- a. Visualizza gli attributi della porta di rete:

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

## Mostra esempio

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

Node: cluster1-02
                                         Speed (Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status

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

Node: cluster1-01
                                         Speed (Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status

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

b. Visualizza 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
```

5. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node   Date          LIF          LIF
Loss
-----
-----
cluster1-01
  3/5/2022 19:21:18 -06:00  cluster1-01_clus2  cluster1-02_clus1
none
  3/5/2022 19:21:20 -06:00  cluster1-01_clus2  cluster1-02_clus2
none

cluster1-02
  3/5/2022 19:21:18 -06:00  cluster1-02_clus2  cluster1-01_clus1
none
  3/5/2022 19:21:20 -06:00  cluster1-02_clus2  cluster1-01_clus2
none
```

## Tutte le versioni ONTAP

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

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

```

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

```

1. Verificare che il auto-revert il comando è abilitato su tutti i LIF del cluster:

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

#### Mostra esempio

```

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

      Logical
Vserver  Interface          Auto-revert
-----
Cluster
      cluster1-01_clus1    true
      cluster1-01_clus2    true
      cluster1-02_clus1    true
      cluster1-02_clus2    true

```

## Cosa succederà ora?

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

## Installa il software NX-OS

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

### Requisiti di revisione

#### Prima di iniziare

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

#### Documentazione suggerita

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

## Installa il software

### Informazioni su questo compito

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

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

#### Passi

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

#### Mostra esempio

```
cs2# ping 172.19.2.1 vrf management
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

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

```
network device-discovery show
```

## Mostra esempio

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
cluster1-01/cdp
      e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
      e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
      e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
      e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*
```

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

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

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

## Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore

          Speed (Mbps)

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

```

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

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

### Mostra esempio

```
cluster1::*> network interface show -role Cluster
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  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    N3K-
C3132Q-V
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        9.3(5)
    Version Source: CDP

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

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

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

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

## Mostra esempio

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password: *****
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

## Mostra esempio

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

```
Software
  BIOS: version 04.25
  NXOS: version 9.3(3)
    BIOS compile time: 01/28/2020
    NXOS image file is: bootflash:///nxos.9.3.3.bin
      NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]
```

```
Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID F0xxxxxxxx23
```

```
Device name: cs2
bootflash: 15137792 kB
usb1: 0 kB (expansion flash)
```

```
Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s):
  cs2#
```

#### 8. Installare l'immagine NX-OS.

L'installazione del file immagine fa sì che questo venga caricato ogni volta che lo switch viene riavviato.

## Mostra esempio

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----  -----
-----  -----
1       yes              Disruptive      Reset         Default
upgrade is not hitless

Images will be upgraded according to following table:
Module      Image      Running-Version(pri:alt)
New-Version  Upg-Required
-----  -----
-----  -----
1          nxos      9.3(3)
9.3(4)          yes
1          bios      v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)  no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading
bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
cs2#
```

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

```
show version
```

## Mostra esempio

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

### Software

```
BIOS: version 04.25
NXOS: version 9.3(4)
BIOS compile time: 05/22/2019
NXOS image file is: bootflash:///nxos.9.3.4.bin
NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]
```

### Hardware

```
cisco Nexus 3132QV Chassis (Nexus 9000 Series)
Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
Processor Board ID FOxxxxxxxx23
```

```
Device name: cs2
bootflash: 15137792 kB
usb1: 0 kB (expansion flash)
```

```
Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s) :

  cs2#
```

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

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

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

## Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
8 entries were displayed.
```

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

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

## Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

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

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

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

cs2                    cluster-network 10.233.205.91      N3K-
```

```
C3132Q-V
```

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

```
2 entries were displayed.
```

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

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

11. Verificare che il cluster sia integro:

```
cluster show
```

#### Mostra esempio

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

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

13. Abilita il ripristino automatico sui LIF del cluster.

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

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

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

#### Mostra esempio

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

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

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

#### Cosa succederà ora?

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

## Installare o aggiornare l'RCF

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

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

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

### Configurazioni RCF disponibili

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

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

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

### RCF disponibili

Nella tabella seguente sono elencati gli RCF disponibili per gli switch 3132Q-V. Scegli la versione RCF applicabile alla tua configurazione. Vedere "[Switch Ethernet Cisco](#)" per maggiori informazioni.

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

### Documentazione suggerita

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

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

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

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

### Informazioni sugli esempi

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

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

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



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

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

### Comandi utilizzati

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

### Cosa succederà ora?

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

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

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

## Prima di iniziare

Verificare le seguenti installazioni e connessioni:

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

## Informazioni su questo compito

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

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

### Fase 1: installare l'RCF sugli switch

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

```
network device-discovery show
```

## Mostra esempio

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
cluster1-01/cdp
      e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
      e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
      e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
      e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*
```

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

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

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

## Mostra esempio

```
cluster1::*> network port show -ipspace Cluster
Node: cluster1-01

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/100000
healthy  false
e0d      Cluster      Cluster          up    9000  auto/100000
healthy  false
Node: cluster1-02

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/100000
healthy  false
e0d      Cluster      Cluster          up    9000  auto/100000
healthy  false
8 entries were displayed.
Node: cluster1-03

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b      Cluster      Cluster          up    9000  auto/10000
healthy  false
Node: cluster1-04

Ignore
                                         Speed (Mbps)
```

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

cluster1::\*>

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

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

#### Mostra esempio

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

cluster1::\*>

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

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

#### Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model
-----
-----
cs1                   cluster-network 10.0.0.1
NX3132QV
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(4)
    Version Source: CDP
cs2                   cluster-network 10.0.0.2
NX3132QV
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(4)
    Version Source: CDP
2 entries were displayed.
```



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

3. Disabilitare il ripristino automatico sui LIF del cluster.

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

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

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

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



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

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

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

#### Mostra esempio

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

6. Verificare che il cluster sia integro:

```
cluster show
```

### Mostra esempio

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

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

```
show running-config
```

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



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

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



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

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

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

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

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

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

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

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

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

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

```
bootflash:write_erase.cfg

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

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

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

14. Riavviare lo switch:

```
cs2# reload
```

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

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

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

## Passaggio 2: verificare le connessioni dello switch

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

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

### Mostra esempio

```
cs1# show interface brief | grep up
.
.
.
Eth1/1/1      1      eth  access  up      none
10G(D)  --
Eth1/1/2      1      eth  access  up      none
10G(D)  --
Eth1/7      1      eth  trunk   up      none
100G(D)  --
Eth1/8      1      eth  trunk   up      none
100G(D)  --
.
.
```

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

```
show port-channel summary
```

### Mostra esempio

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        S - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
-----
-----
Group Port-      Type      Protocol Member Ports
      Channel
-----
1      Po1 (SU)    Eth       LACP      Eth1/31 (P)   Eth1/32 (P)
cs1#
```

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

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

### Mostra esempio

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

#### 4. Verificare che il cluster sia integro:

```
cluster show
```

### Mostra esempio

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

### Passaggio 3: configura il tuo cluster ONTAP

NetApp consiglia di utilizzare System Manager per configurare nuovi cluster.

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

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

#### Cosa succederà ora?

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

#### Aggiorna il tuo file di configurazione di riferimento (RCF)

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

#### Prima di iniziare

Assicurati di avere quanto segue:

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

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

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

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

#### Passaggio 1: Prepararsi all'aggiornamento

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

```
network device-discovery show
```

## Mostra esempio

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
cluster1-01/cdp
      e0a    cs1          Ethernet1/7      N3K-
C3132Q-V
      e0d    cs2          Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
      e0a    cs1          Ethernet1/8      N3K-
C3132Q-V
      e0d    cs2          Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
      e0a    cs1          Ethernet1/1/1    N3K-
C3132Q-V
      e0b    cs2          Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
      e0a    cs1          Ethernet1/1/2    N3K-
C3132Q-V
      e0b    cs2          Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*
```

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

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

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

## Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore

          Speed (Mbps)

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

```

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

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

## Mostra esempio

```
cluster1::*> network interface show -vserver Cluster
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  Port        Home
  -----
  -----
  Cluster
      cluster1-01_clus1  up/up    169.254.3.4/23
  cluster1-01  e0a      true
      cluster1-01_clus2  up/up    169.254.3.5/23
  cluster1-01  e0d      true
      cluster1-02_clus1  up/up    169.254.3.8/23
  cluster1-02  e0a      true
      cluster1-02_clus2  up/up    169.254.3.9/23
  cluster1-02  e0d      true
      cluster1-03_clus1  up/up    169.254.1.3/23
  cluster1-03  e0a      true
      cluster1-03_clus2  up/up    169.254.1.1/23
  cluster1-03  e0b      true
      cluster1-04_clus1  up/up    169.254.1.6/23
  cluster1-04  e0a      true
      cluster1-04_clus2  up/up    169.254.1.7/23
  cluster1-04  e0b      true
cluster1::*>
```

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

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

## Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch          Type          Address
Model
-----
-----
cs1            cluster-network 10.0.0.1
NX3132QV
    Serial Number: 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 10.0.0.2
NX3132QV
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(4)
    Version Source: CDP

2 entries were displayed.
```



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

3. Disabilitare il ripristino automatico sui LIF del cluster.

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

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

## Passaggio 2: configurare le porte

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

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



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

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

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

#### Mostra esempio

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

3. Verificare che il cluster sia integro:

```
cluster show
```

### Mostra esempio

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

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

```
show running-config
```

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

Assicurati di configurare quanto segue:



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

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



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

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

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

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

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

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

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

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

11. Riavviare lo switch:

```
cs2# reload
```

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

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

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

13. Copiare l'RCF nel bootflash dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: FTP, TFTP, SFTP o SCP. Per ulteriori informazioni sui comandi Cisco , consultare la guida appropriata nel "[Riferimento ai comandi NX-OS della serie Cisco Nexus 3000](#)" guide.

#### Mostra esempio

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

#### 14. Applicare l'RCF precedentemente scaricato al bootflash.

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

##### Mostra esempio

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



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

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

```
show running-config
```

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

- Lo striscione RCF
- Le impostazioni del nodo e della porta
- Personalizzazioni

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



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

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

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

##### Mostra esempio

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

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

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

18. Riapplicare eventuali personalizzazioni precedenti alla configurazione dello switch. Fare riferimento a "[Esaminare le considerazioni sul cablaggio e sulla configurazione](#)" per i dettagli di eventuali ulteriori modifiche richieste.
19. Verificare lo stato delle porte del cluster sul cluster.
  - a. Verificare che le porte del cluster siano attive e funzionanti su tutti i nodi del cluster:

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

## Mostra esempio

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

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

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

## Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

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

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

-----
-----
cs1                    cluster-network 10.233.205.90
N3K-C3132Q-V
    Serial Number: FOXXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version
        9.3(4)
    Version Source: CDP

cs2                    cluster-network 10.233.205.91
```

N3K-C3132Q-V

Serial Number: FOXXXXXXXGS

Is Monitored: true

Reason: None

Software Version: Cisco Nexus Operating System (NX-OS)

Software, Version

9.3(4)

Version Source: CDP

2 entries were displayed.

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

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

 2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK\_CONSIST\_PORT: Unblocking port port-channel1 on VLAN0092. Port consistency restored.  
2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK\_PVID\_PEER: Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.  
2020 Nov 17 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK\_PVID\_LOCAL: Blocking port-channel1 on VLAN0092. Inconsistent local vlan.

+

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

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

**Mostra esempio**

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



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

21. Verificare che i LIF del cluster siano stati migrati alle porte ospitate sullo switch cs2. Potrebbero volerci alcuni secondi.

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

**Mostra esempio**

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

22. Verificare che il cluster sia integro:

```
cluster show
```

## Mostra esempio

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

23. Ripetere i passaggi da 1 a 19 sullo switch cs1.
24. Abilita il ripristino automatico sui LIF del cluster.

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

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

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

## Passaggio 3: verificare la configurazione

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

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

### Mostra esempio

```
cs1# show interface brief | grep up
.
.
.
Eth1/1/1      1      eth  access  up      none
10G(D)  --
Eth1/1/2      1      eth  access  up      none
10G(D)  --
Eth1/7      1      eth  trunk   up      none
100G(D)  --
Eth1/8      1      eth  trunk   up      none
100G(D)  --
.
.
```

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

```
show port-channel summary
```

### Mostra esempio

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        S - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
-----
-----
Group Port-      Type      Protocol Member Ports
      Channel
-----
1      Po1 (SU)    Eth       LACP      Eth1/31 (P)   Eth1/32 (P)
cs1#
```

3. Verificare che i LIF del cluster siano tornati alle loro porte home:

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

### Mostra esempio

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

#### 4. Verificare che il cluster sia integro:

```
cluster show
```

### Mostra esempio

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

5. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node   Date          LIF          LIF
Loss
-----
-----
cluster1-01
  3/5/2022 19:21:18 -06:00  cluster1-01_clus2  cluster1-02_clus1
none
  3/5/2022 19:21:20 -06:00  cluster1-01_clus2  cluster1-02_clus2
none

cluster1-02
  3/5/2022 19:21:18 -06:00  cluster1-02_clus2  cluster1-01_clus1
none
  3/5/2022 19:21:20 -06:00  cluster1-02_clus2  cluster1-01_clus2
none
```

## Tutte le versioni ONTAP

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

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

```

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

```

### Cosa succederà ora?

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

## Verifica la tua configurazione SSH

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

### Passi

1. Verificare che SSH sia abilitato:

```

(switch) show ssh server
ssh version 2 is enabled

```

2. Verificare che le chiavi SSH siano abilitate:

```
show ssh key
```

## Mostra esempio

```
(switch) # show ssh key

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

ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAAAgQDiNrD52Q586wTGJjFAbjB1FaA23EpDrZ2sDCew
17nwlioC6HBejxluI0bAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCD Srp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIBmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
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 abilita FIPS, è necessario modificare il bitcount a 256 sullo switch utilizzando il comando `ssh key ecdsa 256 force`. Vedere "["Configurare la sicurezza di rete utilizzando FIPS"](#) per maggiori dettagli.

### Cosa succederà ora?

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

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

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

### Informazioni su questo compito

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

### Passi

1. Cancella la configurazione esistente:

```
write erase
```

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

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

2. Ricaricare il software dello switch:

```
reload
```

```
(cs2) # reload
```

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

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

### Cosa c'è dopo?

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

## Migrare gli switch

### Migrazione da cluster senza switch a cluster con switch a due nodi

#### Flusso di lavoro per la migrazione da cluster switchless a cluster switch a due nodi

Seguire questi passaggi del flusso di lavoro per migrare da un cluster switchless a due nodi a un cluster switch a due nodi che include switch di rete cluster Cisco Nexus 3132Q-V.

1

["Requisiti di migrazione"](#)

Esaminare i requisiti e le informazioni di esempio sullo switch per il processo di migrazione.

2

### "Prepararsi alla migrazione"

Prepara i tuoi cluster switchless per la migrazione a cluster switch a due nodi.

3

### "Configura le tue porte"

Configura le porte per la migrazione da cluster switchless a due nodi a cluster switched a due nodi.

4

### "Completa la tua migrazione"

Completa la migrazione dai cluster switchless ai cluster switch a due nodi.

## Requisiti di migrazione

Se si dispone di un cluster switchless a due nodi, consultare questa procedura per i requisiti applicabili alla migrazione a un cluster switched a due nodi.



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

Per maggiori informazioni, vedere:

- ["NetApp CN1601 e CN1610"](#)
- ["Switch Ethernet Cisco"](#)
- ["Hardware Universe"](#)

## Connessioni di porte e nodi

Quando si esegue la migrazione a un cluster commutato a due nodi con switch cluster Cisco Nexus 3132Q-V, assicurarsi di comprendere i requisiti di collegamento delle porte e dei nodi e di cablaggio.

- Gli switch cluster utilizzano le porte Inter-Switch Link (ISL) e1/31-32.
- Il ["Hardware Universe"](#) contiene informazioni sul cablaggio supportato per gli switch Nexus 3132Q-V:
  - I nodi con connessioni cluster 10 GbE richiedono moduli ottici QSFP con cavi in fibra ottica breakout o cavi breakout in rame da QSFP a SFP+.
  - I nodi con connessioni cluster da 40 GbE richiedono moduli ottici QSFP/QSFP28 supportati con cavi in fibra o cavi di collegamento diretto in rame QSFP/QSFP28.
  - Gli switch cluster utilizzano il cablaggio ISL appropriato: 2 cavi QSFP28 in fibra o rame a collegamento diretto.
- Su Nexus 3132Q-V, è possibile utilizzare le porte QSFP in modalità Ethernet 40 Gb o Ethernet 4x10 Gb.

Per impostazione predefinita, nella modalità Ethernet da 40 Gb sono presenti 32 porte. Queste porte Ethernet da 40 Gb sono numerate secondo una convenzione di denominazione a 2 tuple. Ad esempio, la seconda porta Ethernet da 40 Gb è numerata come 1/2. Il processo di modifica della configurazione da 40 Gb Ethernet a 10 Gb Ethernet è chiamato *breakout*, mentre il processo di modifica della configurazione da 10 Gb Ethernet a 40 Gb Ethernet è chiamato *breakin*. Quando si scomponete una porta Ethernet da 40 Gb in

porte Ethernet da 10 Gb, le porte risultanti vengono numerate utilizzando una convenzione di denominazione a 3 tuple. Ad esempio, le porte breakout della seconda porta Ethernet da 40 Gb sono numerate come 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- Sul lato sinistro del Nexus 3132Q-V è presente un set di quattro porte SFP+ multiplexate sulla prima porta QSFP.

Per impostazione predefinita, l'RCF è strutturato per utilizzare la prima porta QSFP.

È possibile rendere attive quattro porte SFP+ anziché una porta QSFP per Nexus 3132Q-V utilizzando hardware profile front portmode sfp-plus comando. Allo stesso modo, è possibile reimpostare Nexus 3132Q-V per utilizzare una porta QSFP invece di quattro porte SFP+ utilizzando hardware profile front portmode qsfp comando.

- Assicurati di aver configurato alcune porte sul Nexus 3132Q-V per funzionare a 10 GbE o 40 GbE.

È possibile suddividere le prime sei porte in modalità 4x10 GbE utilizzando interface breakout module 1 port 1-6 map 10g-4x comando. Allo stesso modo, è possibile raggruppare le prime sei porte QSFP+ dalla configurazione breakout utilizzando no interface breakout module 1 port 1-6 map 10g-4x comando.

- Il numero di porte 10 GbE e 40 GbE è definito nei file di configurazione di riferimento (RCF) disponibili all'indirizzo "[Download del file di configurazione di riferimento dello switch di rete Cisco ® Cluster](#)" .

## Prima di iniziare

- Configurazioni correttamente impostate e funzionanti.
- Nodi che eseguono ONTAP 9.4 o versioni successive.
- Tutte le porte del cluster nel `up` stato.
- È supportato lo switch cluster Cisco Nexus 3132Q-V.
- La configurazione di rete del cluster esistente presenta:
  - L'infrastruttura del cluster Nexus 3132 è ridondante e completamente funzionale su entrambi gli switch.
  - Le ultime versioni RCF e NX-OS sui tuoi switch.

"[Switch Ethernet Cisco](#)" contiene informazioni sulle versioni ONTAP e NX-OS supportate in questa procedura.

- Connattività di gestione su entrambi gli switch.
- Accesso alla console per entrambi gli switch.
- Tutte le interfacce logiche del cluster (LIF) nel `up` stato senza essere migrato.
- Personalizzazione iniziale dello switch.
- Tutte le porte ISL sono abilitate e cablate.

Inoltre, è necessario pianificare, migrare e leggere la documentazione richiesta sulla connattività 10 GbE e 40 GbE dai nodi agli switch cluster Nexus 3132Q-V.

## Informazioni sugli esempi utilizzati

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

- Switch cluster Nexus 3132Q-V, C1 e C2.

- I nodi sono n1 e n2.



Gli esempi in questa procedura utilizzano due nodi, ciascuno con due porte di interconnessione cluster da 40 GbE **e4a** e **e4e**. Il "Hardware Universe" contiene dettagli sulle porte del cluster sulle tue piattaforme.

Questa procedura copre i seguenti scenari:

- **n1\_clus1** è la prima interfaccia logica del cluster (LIF) da connettere allo switch del cluster C1 per il nodo **n1**.
- **n1\_clus2** è il primo cluster LIF ad essere connesso allo switch del cluster C2 per il nodo **n1**.
- **n2\_clus1** è il primo cluster LIF ad essere connesso allo switch del cluster C1 per il nodo **n2**.
- **n2\_clus2** è il secondo cluster LIF da connettere allo switch cluster C2 per il nodo **n2**.
- Il numero di porte 10 GbE e 40 GbE è definito nei file di configurazione di riferimento (RCF) disponibili all'indirizzo "[Download del file di configurazione di riferimento dello switch di rete Cisco ® Cluster](#)".



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

- Il cluster inizia con due nodi connessi e funzionanti in un ambiente di cluster switchless a due nodi.
- La prima porta del cluster viene spostata su C1.
- La seconda porta del cluster viene spostata su C2.
- L'opzione cluster switchless a due nodi è disabilitata.

### Cosa succederà ora?

Dopo aver esaminato i requisiti di migrazione, puoi "[preparati a migrare i tuoi switch](#)".

### Prepararsi alla migrazione da cluster switchless a cluster switching

Segui questi passaggi per preparare il tuo cluster switchless per la migrazione a un cluster switched a due nodi.

#### Passi

1. Se AutoSupport è abilitato su questo cluster, sopprimere la creazione automatica dei casi richiamando un messaggio AutoSupport :

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

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



Il messaggio AutoSupport avvisa il supporto tecnico di questa attività di manutenzione, in modo che la creazione automatica dei casi venga soppressa durante la finestra di manutenzione.

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

- a. Visualizza gli attributi della porta di rete:

```
network port show
```

## Mostra esempio

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

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

-----
e4a      Cluster      Cluster          up   9000 auto/40000 -
-
e4e      Cluster      Cluster          up   9000 auto/40000 -
-

Node: n2

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

-----
e4a      Cluster      Cluster          up   9000 auto/40000 -
-
e4e      Cluster      Cluster          up   9000 auto/40000 -
-
4 entries were displayed.
```

b. Visualizza informazioni sulle interfacce logiche:

```
network interface show
```

## Mostra esempio

```
cluster::*# network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

3. Verificare che sui nuovi switch 3132Q-V siano installati gli RCF e l'immagine appropriati in base alle proprie esigenze ed effettuare eventuali personalizzazioni essenziali del sito, come utenti e password, indirizzi di rete e così via.

A questo punto è necessario preparare entrambi gli switch. Se è necessario aggiornare il software RCF e quello delle immagini, è necessario seguire questi passaggi:

- Vai a "[Switch Ethernet Cisco](#)" sul sito di supporto NetApp .
  - Annota il tuo switch e le versioni software richieste nella tabella in quella pagina.
  - Scarica la versione appropriata di RCF.
  - Selezionare **CONTINUA** nella pagina **Descrizione**, accettare il contratto di licenza e quindi seguire le istruzioni nella pagina **Download** per scaricare l'RCF.
  - Scarica la versione appropriata del software per le immagini.
4. Selezionare **CONTINUA** nella pagina **Descrizione**, accettare il contratto di licenza e quindi seguire le istruzioni nella pagina **Download** per scaricare l'RCF.

### Cosa succederà ora?

Dopo esserti preparato a migrare i tuoi switch, puoi "[configura le tue porte](#)" .

### Configura le tue porte per la migrazione da cluster switchless a cluster switching

Seguire questi passaggi per configurare le porte per la migrazione da cluster switchless a due nodi a cluster switched a due nodi.

### Passi

1. Sugli switch Nexus 3132Q-V C1 e C2, disabilitare tutte le porte C1 e C2 rivolte al nodo, ma non disabilitare le porte ISL.

#### Mostra esempio

L'esempio seguente mostra le porte da 1 a 30 disabilitate sugli switch cluster Nexus 3132Q-V C1 e C2 utilizzando una configurazione supportata in RCF NX3132\_RCF\_v1.1\_24p10g\_26p40g.txt:

```
C1# copy running-config startup-config
[#####
Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit

C2# copy running-config startup-config
[#####
Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

2. Collegare le porte 1/31 e 1/32 su C1 alle stesse porte su C2 utilizzando il cablaggio supportato.

3. Verificare che le porte ISL siano operative su C1 e C2:

```
show port-channel summary
```

## Mostra esempio

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
```

Group	Port- Channel	Type	Protocol	Member Ports
-------	------------------	------	----------	--------------

1	Pol (SU)	Eth	LACP	Eth1/31 (P)    Eth1/32 (P)
---	----------	-----	------	----------------------------

```
C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
```

Group	Port- Channel	Type	Protocol	Member Ports
-------	------------------	------	----------	--------------

1	Pol (SU)	Eth	LACP	Eth1/31 (P)    Eth1/32 (P)
---	----------	-----	------	----------------------------

## 4. Visualizza l'elenco dei dispositivi vicini sullo 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
C2                  Eth1/31       174      R S I s      N3K-C3132Q-V
Eth1/31
C2                  Eth1/32       174      R S I s      N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

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
C1                  Eth1/31       178      R S I s      N3K-C3132Q-V
Eth1/31
C1                  Eth1/32       178      R S I s      N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

## 5. Visualizza la connettività delle porte del cluster su ciascun nodo:

```
network device-discovery show
```

## Mostra esempio

L'esempio seguente mostra una configurazione di cluster switchless a due nodi.

```
cluster::*> network device-discovery show
      Local   Discovered
      Node    Port   Device        Interface      Platform
      -----  -----  -----
      n1      /cdp
              e4a    n2           e4a          FAS9000
              e4e    n2           e4e          FAS9000
      n2      /cdp
              e4a    n1           e4a          FAS9000
              e4e    n1           e4e          FAS9000
```

## 6. Migrare l'interfaccia clus1 alla porta fisica che ospita clus2:

```
network interface migrate
```

Eseguire questo comando da ciascun nodo locale.

## Mostra esempio

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
      -source-node n1
      -destination-node n1 -destination-port e4e
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
      -source-node n2
      -destination-node n2 -destination-port e4e
```

## 7. Verificare la migrazione delle interfacce del cluster:

```
network interface show
```

## Mostra esempio

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4e      false
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4e      false
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

## 8. Arrestare le porte del cluster clus1 LIF su entrambi i nodi:

```
network port modify
```

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

## 9. Verificare la connettività delle interfacce del cluster remoto:

### ONTAP 9.9.1 e versioni successive

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

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

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

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

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

		Source	Destination	
Packet				
Node	Date	LIF	LIF	
Loss				
-----				
-----				
n1				
	3/5/2022 19:21:18 -06:00	n1_clus2	n2_clus1	none
	3/5/2022 19:21:20 -06:00	n1_clus2	n2_clus2	none
n2				
	3/5/2022 19:21:18 -06:00	n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00	n2_clus2	n1_clus2	none

### Tutte le versioni ONTAP

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

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

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.3
  Local 10.10.0.1 to Remote 10.10.0.4
  Local 10.10.0.2 to Remote 10.10.0.3
  Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
  1 paths up, 0 paths down (tcp check)
  1 paths up, 0 paths down (ucp check)

```

1. Collegare il cavo da e4a sul nodo n1.

È possibile fare riferimento alla configurazione in esecuzione e collegare la prima porta 40 GbE sullo switch C1 (porta 1/7 in questo esempio) a e4a su n1 utilizzando il cablaggio supportato su Nexus 3132Q-V.



Quando si ricollegano i cavi a un nuovo switch cluster Cisco , i cavi utilizzati devono essere in fibra ottica o cavi supportati da Cisco.

2. Collegare il cavo da e4a sul nodo n2.

È possibile fare riferimento alla configurazione in esecuzione e collegare e4a alla successiva porta 40 GbE disponibile su C1, porta 1/8, utilizzando il cablaggio supportato.

3. Abilitare tutte le porte rivolte al nodo su C1.

## Mostra esempio

L'esempio seguente mostra le porte da 1 a 30 abilitate sugli switch cluster Nexus 3132Q-V C1 e C2 utilizzando la configurazione supportata in RCF NX3132\_RCF\_v1.1\_24p10g\_26p40g.txt :

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

4. Abilitare la prima porta del cluster, e4a, su ciascun nodo:

```
network port modify
```

## Mostra esempio

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

5. Verificare che i cluster siano attivi su entrambi i nodi:

```
network port show
```

## Mostra esempio

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
e4a      Cluster      Cluster      up     9000 auto/40000 -
-
e4e      Cluster      Cluster      up     9000 auto/40000 -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
e4a      Cluster      Cluster      up     9000 auto/40000 -
-
e4e      Cluster      Cluster      up     9000 auto/40000 -
-
4 entries were displayed.
```

6. Per ogni nodo, ripristinare tutti i LIF di interconnessione del cluster migrati:

```
network interface revert
```

## Mostra esempio

L'esempio seguente mostra i LIF migrati che vengono ripristinati alle loro porte di origine.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

7. Verificare che tutte le porte di interconnessione del cluster siano ora ripristinate alle loro porte home:

```
network interface show
```

IL Is Home la colonna dovrebbe visualizzare un valore di true per tutte le porte elencate nel Current Port colonna. Se il valore visualizzato è false , la porta non è stata ripristinata.

#### Mostra esempio

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

8. Visualizza la connettività delle porte del cluster su ciascun nodo:

```
network device-discovery show
```

**Mostra esempio**

```
cluster::*> network device-discovery show
      Local   Discovered
      Node    Port   Device           Interface      Platform
-----  -----  -----  -----
-----  -----
n1      /cdp
      e4a    C1           Ethernet1/7   N3K-C3132Q-V
      e4e    n2           e4e          FAS9000
n2      /cdp
      e4a    C1           Ethernet1/8   N3K-C3132Q-V
      e4e    n1           e4e          FAS9000
```

9. Sulla console di ciascun nodo, migrare clus2 sulla porta e4a:

```
network interface migrate
```

**Mostra esempio**

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e4a
```

10. Arrestare le porte del cluster clus2 LIF su entrambi i nodi:

```
network port modify
```

L'esempio seguente mostra le porte specificate che vengono chiuse su entrambi i nodi:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

11. Verificare lo stato LIF del cluster:

```
network interface show
```

## Mostra esempio

```
cluster::*# network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
  e4a      n1_clus1  up/up      10.10.0.1/24      n1
  e4a      true
  e4a      n1_clus2  up/up      10.10.0.2/24      n1
  e4a      false
  e4a      n2_clus1  up/up      10.10.0.3/24      n2
  e4a      true
  e4a      n2_clus2  up/up      10.10.0.4/24      n2
  e4a      false
4 entries were displayed.
```

12. Collegare il cavo da e4e sul nodo n1.

È possibile fare riferimento alla configurazione in esecuzione e collegare la prima porta 40 GbE sullo switch C2 (porta 1/7 in questo esempio) a e4e su n1 utilizzando il cablaggio supportato su Nexus 3132Q-V.

13. Collegare il cavo da e4e sul nodo n2.

È possibile fare riferimento alla configurazione in esecuzione e collegare e4e alla successiva porta 40 GbE disponibile su C2, porta 1/8, utilizzando il cablaggio supportato.

14. Abilitare tutte le porte rivolte verso il nodo su C2.

## Mostra esempio

L'esempio seguente mostra le porte da 1 a 30 abilitate sugli switch cluster Nexus 3132Q-V C1 e C2 utilizzando una configurazione supportata in RCF NX3132\_RCF\_v1.1\_24p10g\_26p40g.txt :

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

15. Abilitare la seconda porta del cluster, e4e, su ciascun nodo:

```
network port modify
```

L'esempio seguente mostra le porte specificate attivate:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> network port modify -node n2 -port e4e -up-admin true
```

16. Per ogni nodo, ripristinare tutti i LIF di interconnessione del cluster migrati:

```
network interface revert
```

L'esempio seguente mostra i LIF migrati che vengono ripristinati alle loro porte di origine.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

17. Verificare che tutte le porte di interconnessione del cluster siano ora ripristinate alle loro porte home:

```
network interface show
```

IL **I**s **H**ome la colonna dovrebbe visualizzare un valore di **true** per tutte le porte elencate nel **C**urrent **P**ort colonna. Se il valore visualizzato è **false** , la porta non è stata ripristinata.

## Mostra esempio

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

18. Verificare che tutte le porte di interconnessione del cluster siano in `up` stato.

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

## Mostra esempio

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
e4a      Cluster      Cluster      up     9000 auto/40000 -
-
e4e      Cluster      Cluster      up     9000 auto/40000 -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
e4a      Cluster      Cluster      up     9000 auto/40000 -
-
e4e      Cluster      Cluster      up     9000 auto/40000 -
-
4 entries were displayed.
```

## Cosa succederà ora?

Dopo aver configurato le porte dello switch, puoi ["completa la tua migrazione"](#) .

## Completere la migrazione da cluster switchless a due nodi a cluster switched a due nodi

Per completare la migrazione da cluster switchless a cluster switched a due nodi, seguire questi passaggi.

### Passi

1. Visualizza i numeri di porta dello switch del cluster a cui è connessa ciascuna porta del cluster su ciascun nodo:

```
network device-discovery show
```

### Mostra esempio

```
cluster::*> network device-discovery show
      Local   Discovered
      Node    Port   Device           Interface      Platform
      -----  -----  -----
      -----
      n1      /cdp
              e4a    C1           Ethernet1/7    N3K-C3132Q-V
              e4e    C2           Ethernet1/7    N3K-C3132Q-V
      n2      /cdp
              e4a    C1           Ethernet1/8    N3K-C3132Q-V
              e4e    C2           Ethernet1/8    N3K-C3132Q-V
```

2. Visualizza gli switch del cluster rilevati e monitorati:

```
system cluster-switch show
```

## Mostra esempio

```
cluster::*> system cluster-switch show

Switch          Type          Address
Model

-----
-----
C1             cluster-network  10.10.1.101
NX3132V
    Serial Number: FOX000001
    Is Monitored: true
    Reason:
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        7.0(3)I4(1)
    Version Source: CDP

C2             cluster-network  10.10.1.102
NX3132V
    Serial Number: FOX000002
    Is Monitored: true
    Reason:
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

3. Disabilitare le impostazioni di configurazione senza switch a due nodi su qualsiasi nodo:

```
network options switchless-cluster
```

```
network options switchless-cluster modify -enabled false
```

4. Verificare che il switchless-cluster l'opzione è stata disabilitata.

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

5. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

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

		Source	Destination	
Packet				
Node	Date	LIF	LIF	
Loss				
-----				
-----				
n1				
	3/5/2022 19:21:18 -06:00	n1_clus2	n2_clus1	none
	3/5/2022 19:21:20 -06:00	n1_clus2	n2_clus2	none
n2				
	3/5/2022 19:21:18 -06:00	n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00	n2_clus2	n1_clus2	none

## Tutte le versioni ONTAP

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

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

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.3
  Local 10.10.0.1 to Remote 10.10.0.4
  Local 10.10.0.2 to Remote 10.10.0.3
  Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
  1 paths up, 0 paths down (tcp check)
  1 paths up, 0 paths down (ucp check)

```

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

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

#### Cosa succederà ora?

Dopo aver completato la migrazione dello switch, puoi ["configurare il monitoraggio dello stato dello switch"](#) .

## Sostituire gli interruttori

### Requisiti per la sostituzione degli switch cluster Cisco Nexus 3132Q-V

Quando si sostituiscono gli switch del cluster, assicurarsi di comprendere i requisiti di configurazione, le connessioni delle porte e i requisiti di cablaggio.

#### Requisiti Cisco Nexus 3132Q-V

- È supportato lo switch cluster Cisco Nexus 3132Q-V.
- Il numero di porte 10 GbE e 40 GbE è definito nei file di configurazione di riferimento (RCF) disponibili all'indirizzo ["Download del file di configurazione di riferimento dello switch di rete Cisco® Cluster"](#) .

- Gli switch cluster utilizzano le porte Inter-Switch Link (ISL) e1/31-32.
- Il "[Hardware Universe](#)" contiene informazioni sul cablaggio supportato per gli switch Nexus 3132Q-V:
  - I nodi con connessioni cluster 10 GbE richiedono moduli ottici QSFP con cavi in fibra ottica breakout o cavi breakout in rame da QSFP a SFP+.
  - I nodi con connessioni cluster da 40 GbE richiedono moduli ottici QSFP/QSFP28 supportati con cavi in fibra o cavi di collegamento diretto in rame QSFP/QSFP28.
  - Gli switch cluster utilizzano il cablaggio ISL appropriato: 2 cavi QSFP28 in fibra o rame a collegamento diretto.
- Su Nexus 3132Q-V, è possibile utilizzare le porte QSFP in modalità Ethernet 40 Gb o Ethernet 4x10 Gb.

Per impostazione predefinita, nella modalità Ethernet da 40 Gb sono presenti 32 porte. Queste porte Ethernet da 40 Gb sono numerate secondo una convenzione di denominazione a 2 tuple. Ad esempio, la seconda porta Ethernet da 40 Gb è numerata come 1/2. Il processo di modifica della configurazione da 40 Gb Ethernet a 10 Gb Ethernet è chiamato *breakout*, mentre il processo di modifica della configurazione da 10 Gb Ethernet a 40 Gb Ethernet è chiamato *breakin*. Quando si scomponete una porta Ethernet da 40 Gb in porte Ethernet da 10 Gb, le porte risultanti vengono numerate utilizzando una convenzione di denominazione a 3 tuple. Ad esempio, le porte breakout della seconda porta Ethernet da 40 Gb sono numerate come 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- Sul lato sinistro del Nexus 3132Q-V è presente un set di quattro porte SFP+ multiplexate sulla prima porta QSFP.

Per impostazione predefinita, l'RCF è strutturato per utilizzare la prima porta QSFP.

È possibile rendere attive quattro porte SFP+ anziché una porta QSFP per Nexus 3132Q-V utilizzando `hardware profile front portmode sfp-plus` comando. Allo stesso modo, è possibile reimpostare Nexus 3132Q-V per utilizzare una porta QSFP invece di quattro porte SFP+ utilizzando `hardware profile front portmode qsfp` comando.

- È necessario aver configurato alcune porte sul Nexus 3132Q-V per funzionare a 10 GbE o 40 GbE.

È possibile suddividere le prime sei porte in modalità 4x10 GbE utilizzando `interface breakout module 1 port 1-6 map 10g-4x` comando. Allo stesso modo, è possibile raggruppare le prime sei porte QSFP+ dalla configurazione breakout utilizzando `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- È necessario aver eseguito la pianificazione, la migrazione e aver letto la documentazione richiesta sulla connettività 10 GbE e 40 GbE dai nodi agli switch cluster Nexus 3132Q-V.

"[Switch Ethernet Cisco](#)" contiene informazioni sulle versioni ONTAP e NX-OS supportate in questa procedura.

## Requisiti Cisco Nexus 5596

- Sono supportati i seguenti switch cluster:
  - Nexus 5596
  - Nexus 3132Q-V
- Il numero di porte 10 GbE e 40 GbE è definito nei file di configurazione di riferimento (RCF) disponibili all'indirizzo "[Download del file di configurazione di riferimento dello switch di rete Cisco® Cluster](#)" .
- Gli switch del cluster utilizzano le seguenti porte per le connessioni ai nodi:

- Porte e1/1-40 (10 GbE): Nexus 5596
- Porte e1/1-30 (40 GbE): Nexus 3132Q-V
- Gli switch del cluster utilizzano le seguenti porte Inter-Switch Link (ISL):
  - Porte e1/41-48 (10 GbE): Nexus 5596
  - Porte e1/31-32 (40 GbE): Nexus 3132Q-V
- IL "[Hardware Universe](#)" contiene informazioni sul cablaggio supportato per gli switch Nexus 3132Q-V:
  - I nodi con connessioni cluster da 10 GbE richiedono cavi breakout in fibra ottica da QSFP a SFP+ o cavi breakout in rame da QSFP a SFP+.
  - I nodi con connessioni cluster da 40 GbE richiedono moduli ottici QSFP/QSFP28 supportati con cavi in fibra o cavi di collegamento diretto in rame QSFP/QSFP28.
- Gli switch del cluster utilizzano il cablaggio ISL appropriato:
  - Inizio: da Nexus 5596 a Nexus 5596 (da SFP+ a SFP+)
    - 8 cavi SFP+ in fibra o rame a collegamento diretto
  - Interim: da Nexus 5596 a Nexus 3132Q-V (break-out da QSFP a 4xSFP+)
    - 1x cavi breakout in fibra QSFP a SFP+ o cavi breakout in rame
  - Finale: da Nexus 3132Q-V a Nexus 3132Q-V (da QSFP28 a QSFP28)
    - 2 cavi QSFP28 in fibra o rame a collegamento diretto
- Sugli switch Nexus 3132Q-V, è possibile utilizzare le porte QSFP/QSFP28 in modalità 40 Gigabit Ethernet o 4 x10 Gigabit Ethernet.

Per impostazione predefinita, nella modalità Ethernet da 40 Gigabit sono presenti 32 porte. Queste 40 porte Gigabit Ethernet sono numerate secondo una convenzione di denominazione a 2 tuple. Ad esempio, la seconda porta Ethernet da 40 Gigabit è numerata come 1/2. Il processo di modifica della configurazione da 40 Gigabit Ethernet a 10 Gigabit Ethernet è chiamato *breakout*, mentre il processo di modifica della configurazione da 10 Gigabit Ethernet a 40 Gigabit Ethernet è chiamato *breakin*. Quando si scomponete una porta Ethernet da 40 Gigabit in porte Ethernet da 10 Gigabit, le porte risultanti vengono numerate utilizzando una convenzione di denominazione a 3 tuple. Ad esempio, le porte break-out della seconda porta Ethernet da 40 Gigabit sono numerate come 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- Sul lato sinistro degli switch Nexus 3132Q-V è presente un set di 4 porte SFP+ multiplexate sulla porta QSFP28.

Per impostazione predefinita, l'RCF è strutturato per utilizzare la porta QSFP28.



È possibile rendere attive 4 porte SFP+ anziché una porta QSFP per gli switch Nexus 3132Q-V utilizzando `hardware profile front portmode sfp-plus` comando. Allo stesso modo, è possibile reimpostare gli switch Nexus 3132Q-V per utilizzare una porta QSFP anziché 4 porte SFP+ utilizzando `hardware profile front portmode qsfp` comando.

- Hai configurato alcune porte sugli switch Nexus 3132Q-V per funzionare a 10 GbE o 40 GbE.



È possibile suddividere le prime sei porte in modalità 4x10 GbE utilizzando `interface breakout module 1 port 1-6 map 10g-4x` comando. Allo stesso modo, è possibile raggruppare le prime sei porte QSFP+ dalla configurazione breakout utilizzando `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Hai eseguito la pianificazione, la migrazione e letto la documentazione richiesta sulla connettività 10 GbE e 40 GbE dai nodi agli switch cluster Nexus 3132Q-V.
- Le versioni ONTAP e NX-OS supportate in questa procedura sono a ["Switch Ethernet Cisco"](#) .

## Requisiti NetApp CN1610

- Sono supportati i seguenti switch cluster:
  - NetApp CN1610
  - Cisco Nexus 3132Q-V
- Gli switch del cluster supportano le seguenti connessioni di nodo:
  - NetApp CN1610: porte da 0/1 a 0/12 (10 GbE)
  - Cisco Nexus 3132Q-V: porte e1/1-30 (40 GbE)
- Gli switch del cluster utilizzano le seguenti porte di collegamento inter-switch (ISL):
  - NetApp CN1610: porte da 0/13 a 0/16 (10 GbE)
  - Cisco Nexus 3132Q-V: porte e1/31-32 (40 GbE)
- IL ["Hardware Universe"](#) contiene informazioni sul cablaggio supportato per gli switch Nexus 3132Q-V:
  - I nodi con connessioni cluster da 10 GbE richiedono cavi breakout in fibra ottica da QSFP a SFP+ o cavi breakout in rame da QSFP a SFP+
  - I nodi con connessioni cluster da 40 GbE richiedono moduli ottici QSFP/QSFP28 supportati con cavi in fibra ottica o cavi di collegamento diretto in rame QSFP/QSFP28
- Il cablaggio ISL appropriato è il seguente:
  - Inizio: per CN1610 a CN1610 (SFP+ a SFP+), quattro cavi SFP+ in fibra ottica o rame a collegamento diretto
  - Interim: per CN1610 a Nexus 3132Q-V (breakout da QSFP a quattro SFP+), un cavo breakout in fibra ottica o rame da QSFP a SFP+
  - Finale: per Nexus 3132Q-V a Nexus 3132Q-V (da QSFP28 a QSFP28), due cavi QSFP28 in fibra ottica o rame a collegamento diretto
- I cavi twinax NetApp non sono compatibili con gli switch Cisco Nexus 3132Q-V.

Se la configurazione CN1610 attuale utilizza cavi twinax NetApp per connessioni cluster-nodo-switch o connessioni ISL e si desidera continuare a utilizzare twinax nel proprio ambiente, è necessario procurarsi cavi twinax Cisco . In alternativa, è possibile utilizzare cavi in fibra ottica sia per le connessioni ISL sia per le connessioni cluster-nodo-switch.

- Sugli switch Nexus 3132Q-V, è possibile utilizzare le porte QSFP/QSFP28 in modalità Ethernet da 40 Gb o Ethernet da 4x 10 Gb.

Per impostazione predefinita, nella modalità Ethernet da 40 Gb sono presenti 32 porte. Queste porte Ethernet da 40 Gb sono numerate secondo una convenzione di denominazione a 2 tuple. Ad esempio, la seconda porta Ethernet da 40 Gb è numerata come 1/2. Il processo di modifica della configurazione da 40 Gb Ethernet a 10 Gb Ethernet è chiamato *breakout*, mentre il processo di modifica della configurazione da 10 Gb Ethernet a 40 Gb Ethernet è chiamato *breakin*. Quando si scomponete una porta Ethernet da 40 Gb in porte Ethernet da 10 Gb, le porte risultanti vengono numerate utilizzando una convenzione di denominazione a 3 tuple. Ad esempio, le porte breakout della seconda porta Ethernet da 40 Gb sono numerate come 1/2/1, 1/2/2, 1/2/3 e 1/2/4.

- Sul lato sinistro degli switch Nexus 3132Q-V è presente un set di quattro porte SFP+ multiplexate sulla prima porta QSFP.

Per impostazione predefinita, il file di configurazione di riferimento (RCF) è strutturato per utilizzare la prima porta QSFP.

È possibile rendere attive quattro porte SFP+ anziché una porta QSFP per gli switch Nexus 3132Q-V utilizzando `hardware profile front portmode sfp-plus` comando. Allo stesso modo, è possibile reimpostare gli switch Nexus 3132Q-V per utilizzare una porta QSFP anziché quattro porte SFP+ utilizzando `hardware profile front portmode qsfp` comando.



Quando si utilizzano le prime quattro porte SFP+, la prima porta QSFP 40GbE verrà disabilitata.

- È necessario aver configurato alcune porte sugli switch Nexus 3132Q-V per funzionare a 10 GbE o 40 GbE.

È possibile suddividere le prime sei porte in modalità 4x10 GbE utilizzando `interface breakout module 1 port 1-6 map 10g-4x` comando. Allo stesso modo, è possibile raggruppare le prime sei porte QSFP+ dalla configurazione `breakout` utilizzando `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- È necessario aver eseguito la pianificazione, la migrazione e aver letto la documentazione richiesta sulla connettività 10 GbE e 40 GbE dai nodi agli switch cluster Nexus 3132Q-V.
- Le versioni ONTAP e NX-OS supportate in questa procedura sono elencate su "[Switch Ethernet Cisco](#)" .
- Le versioni ONTAP e FASTPATH supportate in questa procedura sono elencate su "[Switch NetApp CN1601 e CN1610](#)" .

## Sostituire gli switch cluster Cisco Nexus 3132Q-V

Seguire questa procedura per sostituire uno switch Cisco Nexus 3132Q-V difettoso in una rete cluster. La procedura di sostituzione è una procedura non distruttiva (NDO).

### Requisiti di revisione

#### Requisiti per l'interruttore

Rivedere il "[Requisiti per la sostituzione degli switch cluster Cisco Nexus 3132Q-V](#)" .

#### Prima di iniziare

- La configurazione esistente del cluster e della rete presenta:
  - L'infrastruttura del cluster Nexus 3132Q-V è ridondante e completamente funzionale su entrambi gli switch.
- "Switch Ethernet Cisco" dispone delle ultime versioni RCF e NX-OS per i tuoi switch.
  - Tutte le porte del cluster sono in `up` stato.
  - La connettività di gestione è presente su entrambi gli switch.
  - Tutte le interfacce logiche del cluster (LIF) sono nel `up` stato e sono stati migrati.
- Per lo switch sostitutivo Nexus 3132Q-V, assicurarsi che:

- La connettività della rete di gestione sullo switch sostitutivo è funzionante.
- L'accesso alla console per l'interruttore sostitutivo è pronto.
- L'immagine desiderata del sistema operativo RCF e NX-OS viene caricata sullo switch.
- La personalizzazione iniziale dello switch è completa.
- ["Hardware Universe"](#)

## Abilita la registrazione della console

NetApp consiglia vivamente di abilitare la registrazione della console sui dispositivi utilizzati e di adottare le seguenti misure quando si sostituisce lo switch:

- Lasciare AutoSupport abilitato durante la manutenzione.
- Attivare un AutoSupport di manutenzione prima e dopo la manutenzione per disattivare la creazione di casi per tutta la durata della manutenzione. Vedi questo articolo della Knowledge Base "["SU92: Come sopprimere la creazione automatica dei casi durante le finestre di manutenzione programmata"](#)" per ulteriori dettagli.
- Abilita la registrazione delle sessioni per tutte le sessioni CLI. Per istruzioni su come abilitare la registrazione della sessione, consultare la sezione "Registrazione dell'output della sessione" in questo articolo della Knowledge Base "["Come configurare PuTTY per una connettività ottimale ai sistemi ONTAP"](#)" .

## Sostituire l'interruttore

Questa procedura sostituisce il secondo switch cluster Nexus 3132Q-V CL2 con il nuovo switch 3132Q-V C2.

### Informazioni sugli esempi

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

- n1\_clus1 è la prima interfaccia logica del cluster (LIF) connessa allo switch del cluster C1 per il nodo n1.
- n1\_clus2 è il primo cluster LIF connesso allo switch cluster CL2 o C2, per il nodo n1.
- n1\_clus3 è il secondo LIF connesso allo switch del cluster C2, per il nodo n1.
- n1\_clus4 è il secondo LIF connesso allo switch del cluster CL1, per il nodo n1.
- Il numero di porte 10 GbE e 40 GbE è definito nei file di configurazione di riferimento (RCF) disponibili all'indirizzo "["Download del file di configurazione di riferimento dello switch di rete Cisco® Cluster"](#)" .
- I nodi sono n1, n2, n3 e n4. - Gli esempi in questa procedura utilizzano quattro nodi: due nodi utilizzano quattro porte di interconnessione cluster da 10 GB: e0a, e0b, e0c ed e0d. Gli altri due nodi utilizzano due porte di interconnessione cluster da 40 GB: e4a ed e4e. Vedi il "["Hardware Universe"](#)" per le porte cluster effettive sulle tue piattaforme.

### Informazioni su questo compito

Questa procedura copre il seguente scenario:

- Il cluster inizia con quattro nodi collegati a due switch cluster Nexus 3132Q-V, CL1 e CL2.
- L'interruttore del cluster CL2 deve essere sostituito da C2
  - Su ciascun nodo, i LIF del cluster connessi a CL2 vengono migrati sulle porte del cluster connesse a CL1.
  - Scollegare i cavi da tutte le porte su CL2 e ricollegarli alle stesse porte sullo switch sostitutivo C2.
  - Su ciascun nodo, i LIF del cluster migrato vengono ripristinati.

## Fase 1: Preparazione alla sostituzione

1. Se AutoSupport è abilitato su questo cluster, sopprimere la creazione automatica dei casi richiamando un messaggio AutoSupport :

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

x è la durata della finestra di manutenzione in ore.



Il messaggio AutoSupport avvisa il supporto tecnico di questa attività di manutenzione, in modo che la creazione automatica dei casi venga soppressa durante la finestra di manutenzione.

2. Visualizza informazioni sui dispositivi nella tua configurazione:

```
network device-discovery show
```

### Mostra esempio

```
cluster::> network device-discovery show
      Local   Discovered
      Node    Port    Device           Interface      Platform
-----  -----  -----
-----  -----
n1      /cdp
      e0a    CL1           Ethernet1/1/1    N3K-C3132Q-V
      e0b    CL2           Ethernet1/1/1    N3K-C3132Q-V
      e0c    CL2           Ethernet1/1/2    N3K-C3132Q-V
      e0d    CL1           Ethernet1/1/2    N3K-C3132Q-V
n2      /cdp
      e0a    CL1           Ethernet1/1/3    N3K-C3132Q-V
      e0b    CL2           Ethernet1/1/3    N3K-C3132Q-V
      e0c    CL2           Ethernet1/1/4    N3K-C3132Q-V
      e0d    CL1           Ethernet1/1/4    N3K-C3132Q-V
n3      /cdp
      e4a    CL1           Ethernet1/7     N3K-C3132Q-V
      e4e    CL2           Ethernet1/7     N3K-C3132Q-V
n4      /cdp
      e4a    CL1           Ethernet1/8     N3K-C3132Q-V
      e4e    CL2           Ethernet1/8     N3K-C3132Q-V
```

12 entries were displayed

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

- a. Visualizza gli attributi della porta di rete:

```
network port show
```

## Mostra esempio

```
cluster::*> network port show -role cluster
              (network port show)

Node: n1

Ignore                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
-----  -----
-----  -----
e0a      Cluster      Cluster          up   9000 auto/10000 -
-
e0b      Cluster      Cluster          up   9000 auto/10000 -
-
e0c      Cluster      Cluster          up   9000 auto/10000 -
-
e0d      Cluster      Cluster          up   9000 auto/10000 -
-

Node: n2

Ignore                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
-----  -----
-----  -----
e0a      Cluster      Cluster          up   9000 auto/10000 -
-
e0b      Cluster      Cluster          up   9000 auto/10000 -
-
e0c      Cluster      Cluster          up   9000 auto/10000 -
-
e0d      Cluster      Cluster          up   9000 auto/10000 -
-

Node: n3

Ignore                                         Speed (Mbps)
Health   Health
```

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
<hr/>						
e4a	Cluster	Cluster		up	9000	auto/40000 -
-						
e4e	Cluster	Cluster		up	9000	auto/40000 -
-						

Node: n4

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
<hr/>						
e4a	Cluster	Cluster		up	9000	auto/40000 -
-						
e4e	Cluster	Cluster		up	9000	auto/40000 -
-						

12 entries were displayed.

b. Visualizza informazioni sulle interfacce logiche:

network interface show

### Mostra esempio

```
cluster::*> network interface show -role cluster
(network interface show)

          Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port        Home
-----  -----  -----  -----
-----  -----  -----  -----
Cluster
          n1_clus1  up/up      10.10.0.1/24      n1
e0a      true
          n1_clus2  up/up      10.10.0.2/24      n1
e0b      true
          n1_clus3  up/up      10.10.0.3/24      n1
e0c      true
          n1_clus4  up/up      10.10.0.4/24      n1
e0d      true
          n2_clus1  up/up      10.10.0.5/24      n2
e0a      true
          n2_clus2  up/up      10.10.0.6/24      n2
e0b      true
          n2_clus3  up/up      10.10.0.7/24      n2
e0c      true
          n2_clus4  up/up      10.10.0.8/24      n2
e0d      true
          n3_clus1  up/up      10.10.0.9/24      n3
e0a      true
          n3_clus2  up/up      10.10.0.10/24     n3
e0e      true
          n4_clus1  up/up      10.10.0.11/24     n4
e0a      true
          n4_clus2  up/up      10.10.0.12/24     n4
e0e      true

12 entries were displayed.
```

c. Visualizza le informazioni sugli switch del cluster rilevati:

```
system cluster-switch show
```

## Mostra esempio

```
cluster::> system cluster-switch show

Switch          Type          Address
Model

-----
-----
CL1            cluster-network 10.10.1.101
NX3132V

  Serial Number: FOX000001
  Is Monitored: true
  Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  7.0(3)I4(1)
  Version Source: CDP

CL2            cluster-network 10.10.1.102
NX3132V

  Serial Number: FOX000002
  Is Monitored: true
  Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  7.0(3)I4(1)
  Version Source: CDP

2 entries were displayed.
```

4. Verificare che sul nuovo switch Nexus 3132Q-V siano installati l'RCF e l'immagine appropriati in base alle proprie esigenze ed effettuare eventuali personalizzazioni essenziali del sito.

A questo punto è necessario preparare l'interruttore sostitutivo. Se è necessario aggiornare RCF e immagine, è necessario seguire questi passaggi:

- a. Sul sito di supporto NetApp , vedere "[Switch Ethernet Cisco](#)" .
  - b. Annota il tuo switch e le versioni software richieste nella tabella in quella pagina.
  - c. Scarica la versione appropriata dell'RCF.
  - d. Fare clic su **CONTINUA** nella pagina **Descrizione**, accettare il contratto di licenza e quindi seguire le istruzioni nella pagina **Download** per scaricare l'RCF.
  - e. Scarica la versione appropriata del software per le immagini.
5. Migrare i LIF associati alle porte del cluster connesse allo switch C2:

```
network interface migrate
```

## Mostra esempio

Questo esempio mostra che la migrazione LIF viene eseguita su tutti i nodi:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2  
-source-node n1 -destination-node n1 -destination-port e0a  
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3  
-source-node n1 -destination-node n1 -destination-port e0d  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2  
-source-node n2 -destination-node n2 -destination-port e0a  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3  
-source-node n2 -destination-node n2 -destination-port e0d  
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2  
-source-node n3 -destination-node n3 -destination-port e4a  
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2  
-source-node n4 -destination-node n4 -destination-port e4a
```

## 6. Verifica lo stato del cluster:

```
network interface show
```

## Mostra esempio

```
cluster::*> network interface show -role cluster
(network interface show)

          Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port        Home
-----  -----  -----  -----  -----
-----  -----
Cluster
          Logical      Status      Network      Current
e0a          n1_clus1    up/up      10.10.0.1/24    n1
          true
          n1_clus2    up/up      10.10.0.2/24    n1
e0a          false
          n1_clus3    up/up      10.10.0.3/24    n1
e0d          false
          n1_clus4    up/up      10.10.0.4/24    n1
e0d          true
          n2_clus1    up/up      10.10.0.5/24    n2
e0a          true
          n2_clus2    up/up      10.10.0.6/24    n2
e0a          false
          n2_clus3    up/up      10.10.0.7/24    n2
e0d          false
          n2_clus4    up/up      10.10.0.8/24    n2
e0d          true
          n3_clus1    up/up      10.10.0.9/24    n3
e4a          true
          n3_clus2    up/up      10.10.0.10/24   n3
e4a          false
          n4_clus1    up/up      10.10.0.11/24   n4
e4a          true
          n4_clus2    up/up      10.10.0.12/24   n4
e4a          false
12 entries were displayed.
```

## 7. Disattivare le porte di interconnessione del cluster fisicamente collegate allo switch CL2:

```
network port modify
```

## Mostra esempio

Questo esempio mostra le porte specificate che vengono chiuse su tutti i nodi:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
          Source          Destination          Packet
Node    Date           LIF           LIF           Loss
-----  -----
n1
  3/5/2022 19:21:18 -06:00    n1_clus2    n2_clus1    none
  3/5/2022 19:21:20 -06:00    n1_clus2    n2_clus2    none

n2
  3/5/2022 19:21:18 -06:00    n2_clus2    n1_clus1    none
  3/5/2022 19:21:20 -06:00    n2_clus2    n1_clus2    none

n3
...
...
n4
...
...
```

## Tutte le versioni ONTAP

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

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
```

```
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
Cluster n3_clus1 n4      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.9
  Local 10.10.0.3 to Remote 10.10.0.10
  Local 10.10.0.3 to Remote 10.10.0.11
  Local 10.10.0.3 to Remote 10.10.0.12
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.9
```

```
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

```
Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

1. Spegnere le porte 1/31 e 1/32 su CL1 e lo switch Nexus 3132Q-V attivo:

```
shutdown
```

#### Mostra esempio

Questo esempio mostra le porte ISL 1/31 e 1/32 disattivate sullo switch CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

#### Passaggio 2: configurare le porte

1. Rimuovere tutti i cavi collegati allo switch CL2 del Nexus 3132Q-V e ricollegarli allo switch sostitutivo C2 su tutti i nodi.
2. Rimuovere i cavi ISL dalle porte e1/31 ed e1/32 su CL2 e ricollegarli alle stesse porte sullo switch sostitutivo C2.
3. Attivare le porte ISL 1/31 e 1/32 sullo switch Nexus 3132Q-V CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

4. Verificare che gli ISL siano attivi su CL1:

```
show port-channel
```

Le porte Eth1/31 e Eth1/32 dovrebbero indicare (P) , il che significa che le porte ISL sono attive nel port-channel.

#### Mostra esempio

```
CL1# 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
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
-----
Group Port-      Type   Protocol   Member
Ports
      Channel
-----
1      Po1 (SU)      Eth     LACP      Eth1/31 (P)   Eth1/32 (P)
```

#### 5. Verificare che gli ISL siano attivi su C2:

```
show port-channel summary
```

Le porte Eth1/31 e Eth1/32 dovrebbero indicare (P) , il che significa che entrambe le porte ISL sono attive nel port-channel.

#### Mostra esempio

```
C2# 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
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
-----
Group Port-      Type   Protocol   Member Ports
Ports
      Channel
-----
1      Po1 (SU)      Eth     LACP      Eth1/31 (P)   Eth1/32 (P)
```

6. Su tutti i nodi, richiamare tutte le porte di interconnessione del cluster connesse allo switch Nexus 3132Q-V C2:

```
network port modify
```

**Mostra esempio**

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

7. Per tutti i nodi, ripristinare tutti i LIF di interconnessione del cluster migrati:

```
network interface revert
```

**Mostra esempio**

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
cluster::*> network interface revert -vserver Cluster -lif n3_clus2
cluster::*> network interface revert -vserver Cluster -lif n4_clus2
```

8. Verificare che le porte di interconnessione del cluster siano ora ripristinate alla loro posizione originale:

```
network interface show
```

## Mostra esempio

Questo esempio mostra che tutti i LIF sono stati ripristinati correttamente perché le porte elencate sotto Current Port la colonna ha uno stato di true nel Is Home colonna. Se il Is Home il valore della colonna è false , il LIF non è stato ripristinato.

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1  up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2  up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3  up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4  up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1  up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2  up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3  up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4  up/up      10.10.0.8/24      n2
e0d      true
      n3_clus1  up/up      10.10.0.9/24      n3
e4a      true
      n3_clus2  up/up      10.10.0.10/24      n3
e4e      true
      n4_clus1  up/up      10.10.0.11/24      n4
e4a      true
      n4_clus2  up/up      10.10.0.12/24      n4
e4e      true
12 entries were displayed.
```

## 9. Verificare che le porte del cluster siano connesse:

```
network port show
```

## Mostra esempio

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

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

-----
-----
e0a      Cluster      Cluster      up      9000  auto/10000  -
-
e0b      Cluster      Cluster      up      9000  auto/10000  -
-
e0c      Cluster      Cluster      up      9000  auto/10000  -
-
e0d      Cluster      Cluster      up      9000  auto/10000  -
-
Node: n2

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

-----
-----
e0a      Cluster      Cluster      up      9000  auto/10000  -
-
e0b      Cluster      Cluster      up      9000  auto/10000  -
-
e0c      Cluster      Cluster      up      9000  auto/10000  -
-
e0d      Cluster      Cluster      up      9000  auto/10000  -
-
Node: n3

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

```

Status
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

Node: n4

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-
12 entries were displayed.

```

10. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
          Source          Destination          Packet
Node    Date           LIF           LIF           Loss
-----  -----
n1
  3/5/2022 19:21:18 -06:00  n1_clus2  n2_clus1  none
  3/5/2022 19:21:20 -06:00  n1_clus2  n2_clus2  none

n2
  3/5/2022 19:21:18 -06:00  n2_clus2  n1_clus1  none
  3/5/2022 19:21:20 -06:00  n2_clus2  n1_clus2  none

n3
...
...
n4
...
...
```

## Tutte le versioni ONTAP

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

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
```

```
Cluster n3_clus1 n3      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.9
  Local 10.10.0.3 to Remote 10.10.0.10
  Local 10.10.0.3 to Remote 10.10.0.11
  Local 10.10.0.3 to Remote 10.10.0.12
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.9
  Local 10.10.0.4 to Remote 10.10.0.10
  Local 10.10.0.4 to Remote 10.10.0.11
```

Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)

RPC status:

8 paths up, 0 paths down (tcp check)

8 paths up, 0 paths down (udp check)

### Passaggio 3: verificare la configurazione

1. Visualizza le informazioni sui dispositivi nella tua configurazione:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

## Mostra esempio

```
cluster::> network device-discovery show
      Local  Discovered
      Node    Port   Device
-----  -----
-----  -----
n1      /cdp
      e0a    C1      Ethernet1/1/1  N3K-C3132Q-V
      e0b    C2      Ethernet1/1/1  N3K-C3132Q-V
      e0c    C2      Ethernet1/1/2  N3K-C3132Q-V
      e0d    C1      Ethernet1/1/2  N3K-C3132Q-V
n2      /cdp
      e0a    C1      Ethernet1/1/3  N3K-C3132Q-V
      e0b    C2      Ethernet1/1/3  N3K-C3132Q-V
      e0c    C2      Ethernet1/1/4  N3K-C3132Q-V
      e0d    C1      Ethernet1/1/4  N3K-C3132Q-V
n3      /cdp
      e4a    C1      Ethernet1/7   N3K-C3132Q-V
      e4e    C2      Ethernet1/7   N3K-C3132Q-V
n4      /cdp
      e4a    C1      Ethernet1/8   N3K-C3132Q-V
      e4e    C2      Ethernet1/8   N3K-C3132Q-V
12 entries were displayed.
```

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore                                         Speed(Mbps)  Health
Health
Port      IPspace      Broadcast  Domain  Link MTU  Admin/Oper  Status
Status
-----  -----
-----  -----
e0a      Cluster      Cluster      up      9000  auto/10000  -
-
e0b      Cluster      Cluster      up      9000  auto/10000  -
-
e0c      Cluster      Cluster      up      9000  auto/10000  -
-
e0d      Cluster      Cluster      up      9000  auto/10000  -
```

Node: n2

Ignore

Health	Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Speed (Mbps) Health
-	e0a	Cluster	Cluster		up	9000	auto/10000	-
-	e0b	Cluster	Cluster		up	9000	auto/10000	-
-	e0c	Cluster	Cluster		up	9000	auto/10000	-
-	e0d	Cluster	Cluster		up	9000	auto/10000	-
-								

Node: n3

Ignore

Health	Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Speed (Mbps) Health
-	e4a	Cluster	Cluster		up	9000	auto/40000	-
-	e4e	Cluster	Cluster		up	9000	auto/40000	-
-								

Node: n4

Ignore

Health	Port Status	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Speed (Mbps) Health
-	e4a	Cluster	Cluster		up	9000	auto/40000	-
-	e4e	Cluster	Cluster		up	9000	auto/40000	-
-								

12 entries were displayed.

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
----- Cluster
e0a          n1_clus1  up/up      10.10.0.1/24      n1
e0b          n1_clus2  up/up      10.10.0.2/24      n1
e0c          n1_clus3  up/up      10.10.0.3/24      n1
e0d          n1_clus4  up/up      10.10.0.4/24      n1
e0a          n2_clus1  up/up      10.10.0.5/24      n2
e0b          n2_clus2  up/up      10.10.0.6/24      n2
e0c          n2_clus3  up/up      10.10.0.7/24      n2
e0d          n2_clus4  up/up      10.10.0.8/24      n2
e4a          n3_clus1  up/up      10.10.0.9/24      n3
e4e          n3_clus2  up/up      10.10.0.10/24     n3
e4a          n4_clus1  up/up      10.10.0.11/24     n4
e4e          n4_clus2  up/up      10.10.0.12/24     n4
12 entries were displayed.
```

```

cluster::*> system cluster-switch show

Switch          Type          Address
Model

-----
CL1            cluster-network 10.10.1.101
NX3132V
    Serial Number: FOX000001
    Is Monitored: true
    Reason:
        Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        7.0(3)I4(1)
    Version Source: CDP

CL2            cluster-network 10.10.1.102
NX3132V
    Serial Number: FOX000002
    Is Monitored: true
    Reason:
        Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        7.0(3)I4(1)
    Version Source: CDP

C2             cluster-network 10.10.1.103
NX3132V
    Serial Number: FOX000003
    Is Monitored: true
    Reason:
        Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        7.0(3)I4(1)
    Version Source: CDP

3 entries were displayed.

```

2. Rimuovere lo switch Nexus 3132Q-V sostituito, se non è già stato rimosso automaticamente:

```
system cluster-switch delete
```

```
cluster::*> system cluster-switch delete -device CL2
```

3. Verificare che siano monitorati gli switch del cluster appropriati:

```
system cluster-switch show
```

#### Mostra esempio

```
cluster::> system cluster-switch show

  Switch          Type          Address
Model

-----
-----
CL1           cluster-network  10.10.1.101
NX3132V

  Serial Number: FOX000001
  Is Monitored: true
  Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  7.0(3)I4(1)
  Version Source: CDP

  C2           cluster-network  10.10.1.103
NX3132V

  Serial Number: FOX000002
  Is Monitored: true
  Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  7.0(3)I4(1)
  Version Source: CDP

2 entries were displayed.
```

4. Se hai disattivato la creazione automatica dei casi, riattiva richiamando un messaggio AutoSupport :

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

#### Cosa succederà ora?

Dopo aver sostituito l'interruttore, puoi ["configurare il monitoraggio dello stato dello switch"](#) .

### Sostituisci gli switch cluster Cisco Nexus 3132Q-V con connessioni switchless

In ONTAP 9.3 e versioni successive, è possibile migrare da un cluster con una rete di cluster commutata a uno in cui due nodi sono connessi direttamente.

NetApp consiglia di aggiornare la versione ONTAP prima di procedere con il passaggio da un cluster switchless a uno switch per gli switch Cisco Nexus 3132Q-V.

Per maggiori dettagli vedere quanto segue:

- "SU540: gli errori della scheda di rete Chelsio T6 causano l'arresto del sistema durante l'aggiornamento da switch di rete da 40G a 100G"
- "Nodo in panico dopo la migrazione da un cluster commutato a uno senza commutazione"

È possibile migrare da un cluster con una rete di cluster commutata a uno in cui due nodi sono collegati direttamente per ONTAP 9.3 e versioni successive.

## Requisiti di revisione

### Linee guida

Rivedere le seguenti linee guida:

- La migrazione a una configurazione cluster switchless a due nodi è un'operazione non distruttiva. La maggior parte dei sistemi ha due porte di interconnessione cluster dedicate su ciascun nodo, ma è possibile utilizzare questa procedura anche per sistemi con un numero maggiore di porte di interconnessione cluster dedicate su ciascun nodo, ad esempio quattro, sei o otto.
- Non è possibile utilizzare la funzionalità di interconnessione del cluster senza switch con più di due nodi.
- Se si dispone di un cluster a due nodi esistente che utilizza switch di interconnessione cluster ed esegue ONTAP 9.3 o versione successiva, è possibile sostituire gli switch con connessioni dirette back-to-back tra i nodi.

### Prima di iniziare

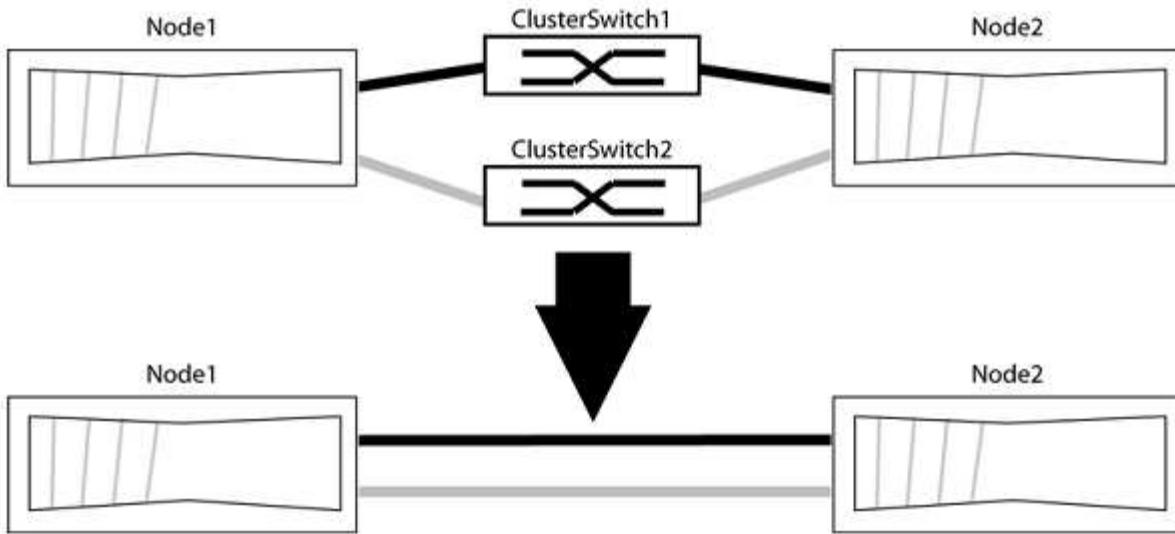
Assicurati di avere quanto segue:

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

## Migrare gli switch

### Informazioni su questo compito

La seguente procedura rimuove gli switch del cluster in un cluster a due nodi e sostituisce ogni connessione allo switch con una connessione diretta al nodo partner.



### Informazioni sugli esempi

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

#### Fase 1: Prepararsi alla migrazione

1. Cambia il livello di privilegio in avanzato, inserendo `y` quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato `*>` appare.

2. ONTAP 9.3 e versioni successive supportano il rilevamento automatico dei cluster switchless, abilitato per impostazione predefinita.

È possibile verificare che il rilevamento dei cluster switchless sia abilitato eseguendo il comando con privilegi avanzati:

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

#### Mostra esempio

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

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

Se "Abilita rilevamento cluster senza switch" è `false`, contattare l'assistenza NetApp .

3. Se AutoSupport è abilitato su questo cluster, sopprimere la creazione automatica dei casi richiamando un messaggio AutoSupport :

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

Dove h è la durata della finestra di manutenzione in ore. Il messaggio avvisa il supporto tecnico di questa attività di manutenzione, in modo che possa sopprimere la creazione automatica dei casi durante la finestra di manutenzione.

Nell'esempio seguente, il comando sopprime la creazione automatica dei casi per due ore:

#### Mostra esempio

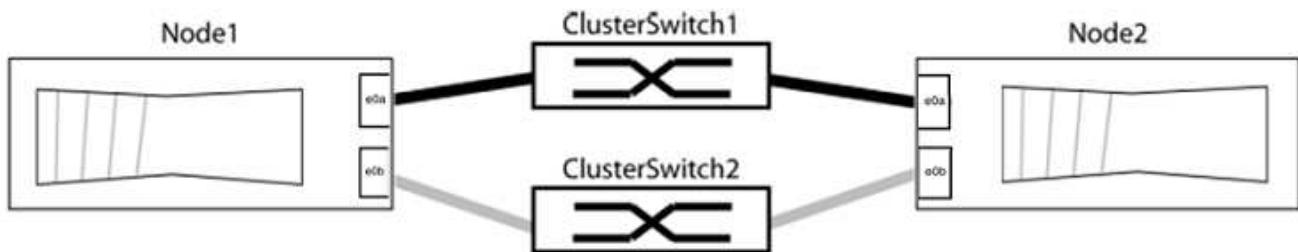
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

#### Passaggio 2: configurare porte e cablaggio

1. Organizzare le porte del cluster su ogni switch in gruppi in modo che le porte del cluster nel gruppo 1 vadano al cluster switch 1 e le porte del cluster nel gruppo 2 vadano al cluster switch 2. Questi gruppi saranno necessari più avanti nella procedura.
2. Identificare le porte del cluster e verificare lo stato e l'integrità del collegamento:

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

Nell'esempio seguente per i nodi con porte cluster "e0a" e "e0b", un gruppo è identificato come "nodo1:e0a" e "nodo2:e0a" e l'altro gruppo come "nodo1:e0b" e "nodo2:e0b". I nodi potrebbero utilizzare porte cluster diverse perché variano in base al sistema.



Verificare che le porte abbiano un valore di `up` per la colonna "Link" e un valore di `healthy` per la colonna "Stato di salute".

## Mostra esempio

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

4 entries were displayed.
```

3. Verificare che tutti i LIF del cluster siano sulle rispettive porte home.

Verificare che la colonna "is-home" sia true per ciascuno dei LIF del cluster:

```
network interface show -vserver Cluster -fields is-home
```

## Mostra esempio

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif      is-home
-----
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Se sono presenti LIF del cluster che non si trovano sulle loro porte home, ripristinare tali LIF sulle loro porte home:

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

4. Disabilitare il ripristino automatico per i LIF del cluster:

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

5. Verificare che tutte le porte elencate nel passaggio precedente siano connesse a uno switch di rete:

```
network device-discovery show -port cluster_port
```

La colonna "Dispositivo rilevato" dovrebbe contenere il nome dello switch del cluster a cui è connessa la porta.

## Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono collegate correttamente agli switch del cluster "cs1" e "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/  Local  Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
      e0a    cs1
      e0b    cs2
node2/cdp
      e0a    cs1
      e0b    cs2
4 entries were displayed.
```

6. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

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

		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 versioni ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verificare che il cluster sia integro:

```
cluster ring show
```

Tutte le unità devono essere master o secondarie.

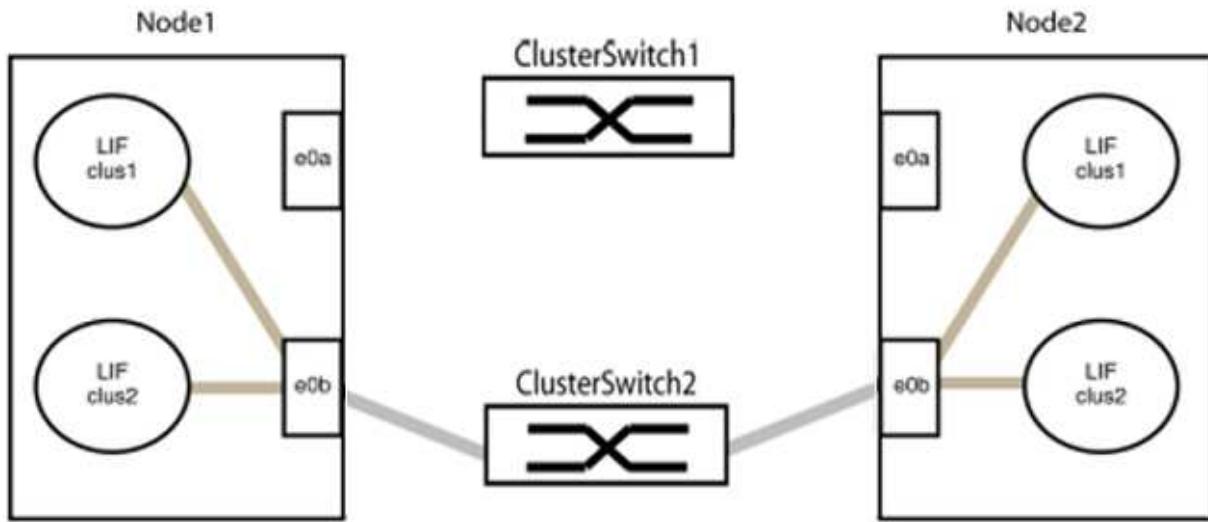
2. Impostare la configurazione senza switch per le porte del gruppo 1.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 1 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

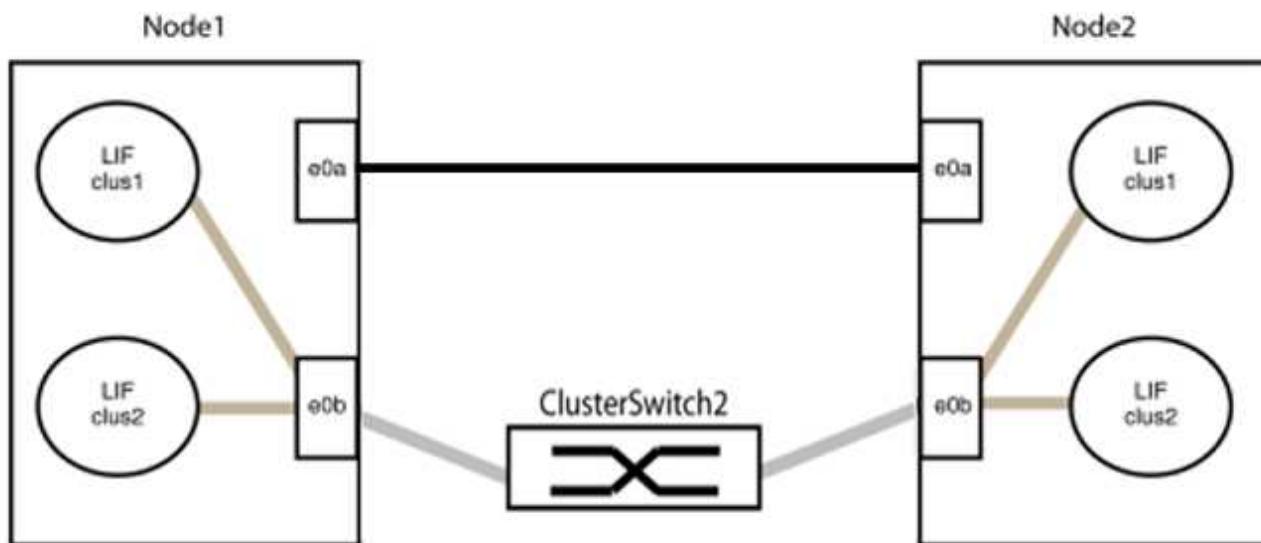
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 1.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0a" su ciascun nodo e il traffico del cluster continua attraverso lo switch e la porta "e0b" su ciascun nodo:



- b. Collegare le porte del gruppo 1 una dietro l'altra.

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



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

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

L'esempio seguente mostra che il cluster switchless è abilitato:

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

4. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

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

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

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

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```



Prima di procedere al passaggio successivo, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

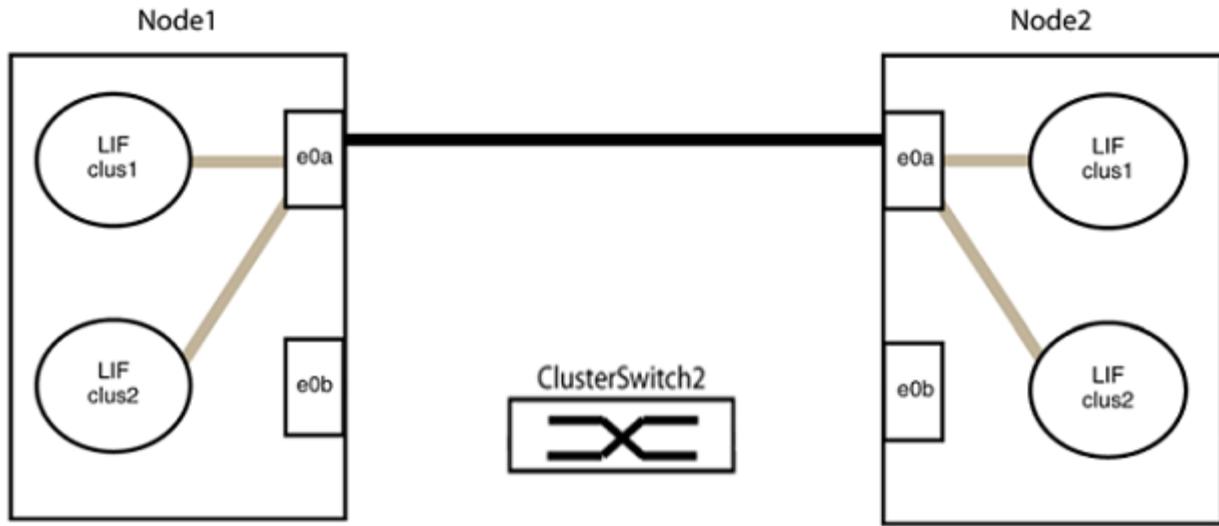
1. Impostare la configurazione senza switch per le porte nel gruppo 2.



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

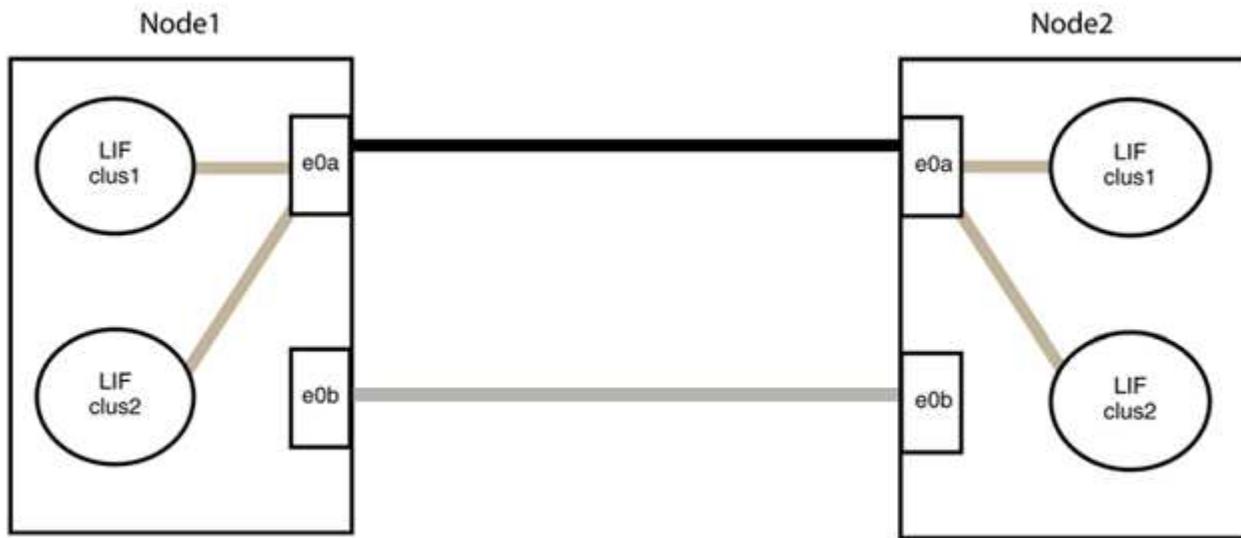
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 2.

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



b. Cablare le porte del gruppo 2 una dietro l'altra.

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



### Passaggio 3: verificare la configurazione

1. Verificare che le porte su entrambi i nodi siano collegate correttamente:

```
network device-discovery show -port cluster_port
```

## Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono correttamente collegate alla porta corrispondente sul partner del cluster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface  Platform
-----  -----  -----  -----  -----  -----
node1/cdp
      e0a    node2
      e0b    node2
node1/lldp
      e0a    node2 (00:a0:98:da:16:44)  e0a
      e0b    node2 (00:a0:98:da:16:44)  e0b
node2/cdp
      e0a    node1
      e0b    node1
node2/lldp
      e0a    node1 (00:a0:98:da:87:49)  e0a
      e0b    node1 (00:a0:98:da:87:49)  e0b
8 entries were displayed.
```

## 2. Riattivare il ripristino automatico per i LIF del cluster:

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

## 3. Verificare che tutti i LIF siano a casa. Potrebbero volerci alcuni secondi.

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

## Mostra esempio

I LIF sono stati ripristinati se la colonna "È a casa" è true , come mostrato per node1\_clus2 E node2\_clus2 nell'esempio seguente:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver    lif          curr-port is-home
-----
Cluster  node1_clus1  e0a        true
Cluster  node1_clus2  e0b        true
Cluster  node2_clus1  e0a        true
Cluster  node2_clus2  e0b        true
4 entries were displayed.
```

Se uno qualsiasi dei LIFS del cluster non è tornato alle proprie porte home, ripristinarlo manualmente dal nodo locale:

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

4. Controllare lo stato del cluster dei nodi dalla console di sistema di uno dei due nodi:

```
cluster show
```

## Mostra esempio

L'esempio seguente mostra epsilon su entrambi i nodi da false :

```
Node  Health  Eligibility Epsilon
-----
node1 true    true        false
node2 true    true        false
2 entries were displayed.
```

5. Verificare la connettività delle interfacce del cluster remoto:

## ONTAP 9.9.1 e versioni successive

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

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

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

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

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

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

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

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

Per maggiori informazioni, vedere "[Articolo 1010449 della Knowledge Base NetApp : Come sopprimere la creazione automatica di casi durante le finestre di manutenzione programmata](#)".

2. Ripristinare il livello di privilegio su amministratore:

```
set -privilege admin
```

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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