



Cisco Nexus 3232C

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-systems-switches/switch-cisco-3232c/install-overview-cisco-3232c.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Cisco Nexus 3232C	1
Iniziare	1
Flusso di lavoro di installazione e configurazione per gli switch Cisco Nexus 3232C	1
Requisiti di configurazione per gli switch Cisco Nexus 3232C	1
Requisiti di documentazione per gli switch Cisco Nexus 3232C	2
Requisiti di Smart Call Home	4
Installare l'hardware	4
Flusso di lavoro di installazione hardware per gli switch Cisco Nexus 3232C	4
Foglio di lavoro completo sul cablaggio Cisco Nexus 3232C	5
Installare lo switch cluster 3232C	8
Installare uno switch cluster Cisco Nexus 3232C 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 3232C	14
Configurare lo switch cluster 3232C	14
Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento (RCF)	17
Installa il software NX-OS	23
Installare o aggiornare l'RCF	43
Verifica la tua configurazione SSH	74
Ripristinare lo switch del cluster 3232C ai valori predefiniti di fabbrica	76
Migrare gli switch	76
Migrazione da cluster switchless a due nodi	76
Sostituire gli interruttori	98
Sostituire uno switch cluster Cisco Nexus 3232C	98
Sostituisci gli switch cluster Cisco Nexus 3232C con connessioni switchless	125
Switch di archiviazione Cisco 3232C	140
Sostituire uno switch di archiviazione Cisco Nexus 3232C	140

Cisco Nexus 3232C

Iniziare

Flusso di lavoro di installazione e configurazione per gli switch Cisco Nexus 3232C

Gli switch Cisco Nexus 3232C 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 3232C.

1

"Requisiti di configurazione"

Esaminare i requisiti di configurazione per lo switch cluster 3232C.

2

"Documentazione richiesta"

Consultare la documentazione specifica dello switch e del controller per configurare gli switch 3232C 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 3232C

Per l'installazione e la manutenzione dello switch Cisco Nexus 3232C, assicurarsi di rivedere la configurazione e i requisiti di rete.

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

Requisiti di documentazione per gli switch Cisco Nexus 3232C

Per l'installazione e la manutenzione dello switch Cisco Nexus 3232C, assicurarsi di consultare tutta la documentazione consigliata.

Documentazione dello switch

Per configurare gli switch Cisco Nexus 3232C, 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 (scegli la guida per la versione NX-OS installata sugli switch)</i>	Fornisce le informazioni di configurazione iniziale dello switch necessarie prima di poterlo configurare per il funzionamento ONTAP .
<i>Guida all'aggiornamento e al downgrade del software Cisco Nexus serie NX-OS (scegli la guida per la versione NX-OS installata sui tuoi switch)</i>	Fornisce informazioni su come effettuare il downgrade dello switch al software dello switch supportato ONTAP , se necessario.
<i>Indice principale di riferimento dei comandi NX-OS della serie Cisco Nexus 3000</i>	Fornisce collegamenti ai vari riferimenti ai comandi forniti da Cisco.

Titolo del documento	Descrizione
<i>Riferimento MIB Cisco Nexus 3000</i>	Descrive i file MIB (Management Information Base) per gli switch Nexus 3000.
<i>Riferimento ai messaggi di sistema NX-OS della serie Nexus 3000</i>	Descrive 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>	Descrive 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	Descrive come installare l'hardware NetApp .
Documentazione ONTAP	Fornisce informazioni dettagliate su tutti gli aspetti delle versioni ONTAP .
"Hardware Universe"	Fornisce informazioni sulla configurazione hardware e sulla compatibilità NetApp .

Documentazione del kit ferroviario e dell'armadio

Per installare uno switch Cisco 3232C in un cabinet NetApp , consultare la seguente documentazione hardware.

Nome	Descrizione
"Armadio di sistema 42U, guida profonda"	Descrive le FRU associate al cabinet del sistema 42U e fornisce istruzioni per la manutenzione e la sostituzione delle FRU.
"Installare uno switch Cisco Nexus 3232C in un cabinet NetApp"	Descrive come installare uno switch Cisco Nexus 3232C 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 3232C

Per installare e configurare l'hardware per uno switch cluster 3232C, 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 3232C.

3

"Installare lo switch in un cabinet NetApp"

Installare lo switch 3232C e il pannello pass-through in un cabinet NetApp secondo necessità.

Esaminare il supporto per le porte Ethernet NVIDIA .

Foglio di lavoro completo sul cablaggio Cisco Nexus 3232C

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 da 100 GbE, 40 GbE o 4 porte da 10 GbE.

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 4x10GbE/4x25GbE o 40/100GbE	1	Nodo 4x10GbE/4x25GbE o 40/100GbE
2	Nodo 4x10GbE/4x25GbE o 40/100GbE	2	Nodo 4x10GbE/4x25GbE o 40/100GbE
3	Nodo 4x10GbE/4x25GbE o 40/100GbE	3	Nodo 4x10GbE/4x25GbE o 40/100GbE
4	Nodo 4x10GbE/4x25GbE o 40/100GbE	4	Nodo 4x10GbE/4x25GbE o 40/100GbE
5	Nodo 4x10GbE/4x25GbE o 40/100GbE	5	Nodo 4x10GbE/4x25GbE o 40/100GbE
6	Nodo 4x10GbE/4x25GbE o 40/100GbE	6	Nodo 4x10GbE/4x25GbE o 40/100GbE
7	Nodo 4x10GbE/4x25GbE o 40/100GbE	7	Nodo 4x10GbE/4x25GbE o 40/100GbE
8	Nodo 4x10GbE/4x25GbE o 40/100GbE	8	Nodo 4x10GbE/4x25GbE o 40/100GbE
9	Nodo 4x10GbE/4x25GbE o 40/100GbE	9	Nodo 4x10GbE/4x25GbE o 40/100GbE

Interruttore del cluster A		Interruttore del cluster B	
10	Nodo 4x10GbE/4x25GbE o 40/100GbE	10	Nodo 4x10GbE/4x25GbE o 40/100GbE
11	Nodo 4x10GbE/4x25GbE o 40/100GbE	11	Nodo 4x10GbE/4x25GbE o 40/100GbE
12	Nodo 4x10GbE/4x25GbE o 40/100GbE	12	Nodo 4x10GbE/4x25GbE o 40/100GbE
13	Nodo 4x10GbE/4x25GbE o 40/100GbE	13	Nodo 4x10GbE/4x25GbE o 40/100GbE
14	Nodo 4x10GbE/4x25GbE o 40/100GbE	14	Nodo 4x10GbE/4x25GbE o 40/100GbE
15	Nodo 4x10GbE/4x25GbE o 40/100GbE	15	Nodo 4x10GbE/4x25GbE o 40/100GbE
16	Nodo 4x10GbE/4x25GbE o 40/100GbE	16	Nodo 4x10GbE/4x25GbE o 40/100GbE
17	Nodo 4x10GbE/4x25GbE o 40/100GbE	17	Nodo 4x10GbE/4x25GbE o 40/100GbE
18	Nodo 4x10GbE/4x25GbE o 40/100GbE	18	Nodo 4x10GbE/4x25GbE o 40/100GbE
19	Nodo 40G/100GbE 19	19	Nodo 40G/100GbE 19
20	Nodo 40G/100GbE 20	20	Nodo 40G/100GbE 20
21	Nodo 21 40G/100GbE	21	Nodo 21 40G/100GbE
22	Nodo 22 40G/100GbE	22	Nodo 22 40G/100GbE
23	Nodo 23 40G/100GbE	23	Nodo 23 40G/100GbE
24	Nodo 40G/100GbE 24	24	Nodo 40G/100GbE 24
25-30	Prenotato	25-30	Prenotato
31	100GbE ISL per commutare la porta B 31	31	100GbE ISL per commutare la porta A 31

Interruttore del cluster A		Interruttore del cluster B	
32	100GbE ISL per commutare la porta B 32	32	100GbE 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	
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	

Interruttore del cluster A		Interruttore del cluster B	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25-30	Prenotato	25-30	Prenotato
31	100GbE ISL per commutare la porta B 31	31	100GbE ISL per commutare la porta A 31
32	100GbE ISL per commutare la porta B 32	32	100GbE ISL per commutare la porta A 32

Cosa c'è dopo?

Dopo aver completato i fogli di lavoro sui cavi, puoi ["installare l'interruttore"](#).

Installare lo switch cluster 3232C

Seguire questa procedura per impostare e configurare lo switch Cisco Nexus 3232C.

Prima di iniziare

Assicurati di avere quanto segue:

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

Passi

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

Se stai installando...	Poi...
Cisco Nexus 3232C 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 3232C e di un pannello pass-through in un cabinet NetApp .
Apparecchiature in un rack Telco	Consultare le procedure fornite nelle guide all'installazione dell'hardware dello switch e nelle istruzioni di installazione e configurazione NetApp .

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

Cosa succederà ora?

Facoltativamente, puoi ["installare uno switch Cisco Nexus 3223C in un cabinet NetApp"](#). Altrimenti vai a ["rivedere il cablaggio e la configurazione"](#).

Installare uno switch cluster Cisco Nexus 3232C in un cabinet NetApp

A seconda della configurazione, potrebbe essere necessario installare lo switch cluster Cisco Nexus 3232C 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"](#) .
- Per ogni switch, le otto viti 10-32 o 12-24 e i 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 .

Il kit del pannello passante è disponibile presso NetApp (codice articolo X8784-R6).

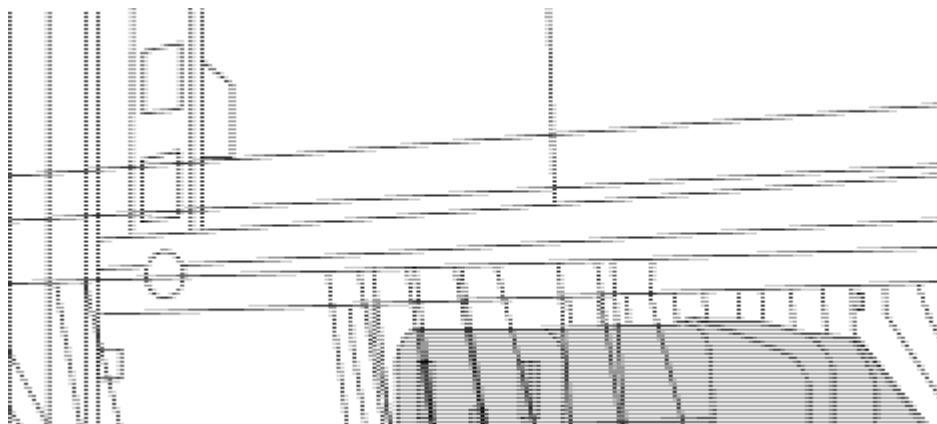
Il kit del pannello pass-through NetApp contiene il seguente hardware:

- Un pannello cieco passante
- Quattro viti 10-32 x .75
- Quattro dadi a clip 10-32

- i. Determinare la posizione verticale degli interruttori e del pannello cieco nell'armadio.

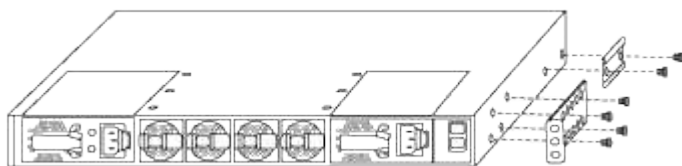
In questa procedura, il pannello cieco verrà installato in U40.

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

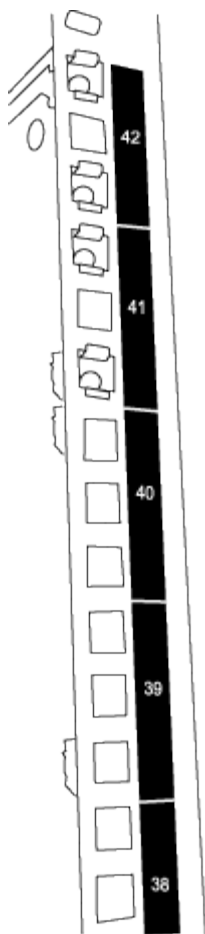


(1) Connettore femmina del cavo di collegamento.

1. Installare le staffe di montaggio su rack sullo chassis dello switch Nexus 3232C.
 - 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.



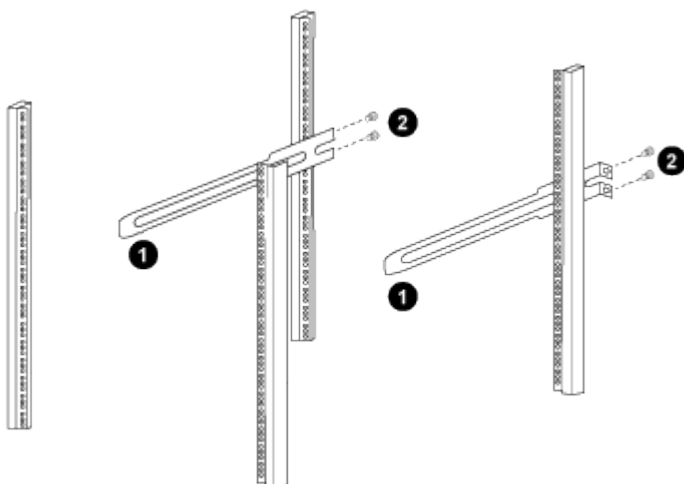
- b. Ripetere il passaggio 2a con l'altra staffa di montaggio su rack anteriore sull'altro lato dello switch.
 - c. Installare la staffa di montaggio posteriore sul telaio dello switch.
 - d. Ripetere il passaggio 2c con l'altra staffa di montaggio su rack posteriore sull'altro lato dello switch.
2. Installare i dadi a clip nelle posizioni dei fori quadrati per tutti e quattro i pali IEA.



I due switch 3232C saranno sempre montati nella parte superiore 2U dell'armadio RU41 e 42.

3. 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) Stringi le viti delle guide scorrevoli ai montanti del mobile.

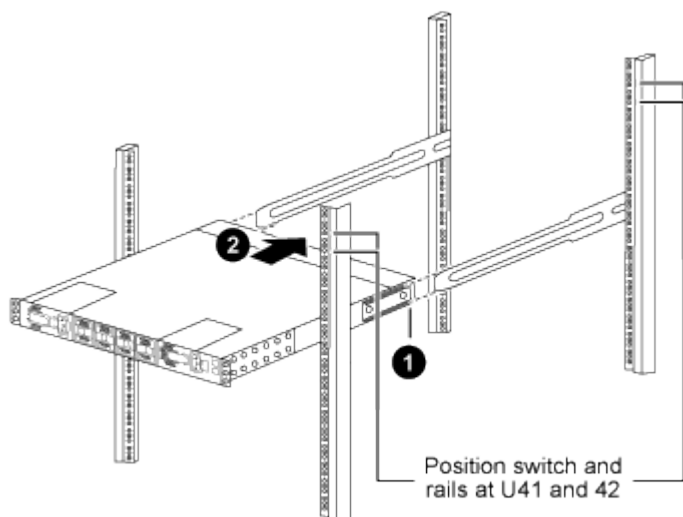
- a. Ripetere il passaggio 4a per il montante posteriore destro.

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

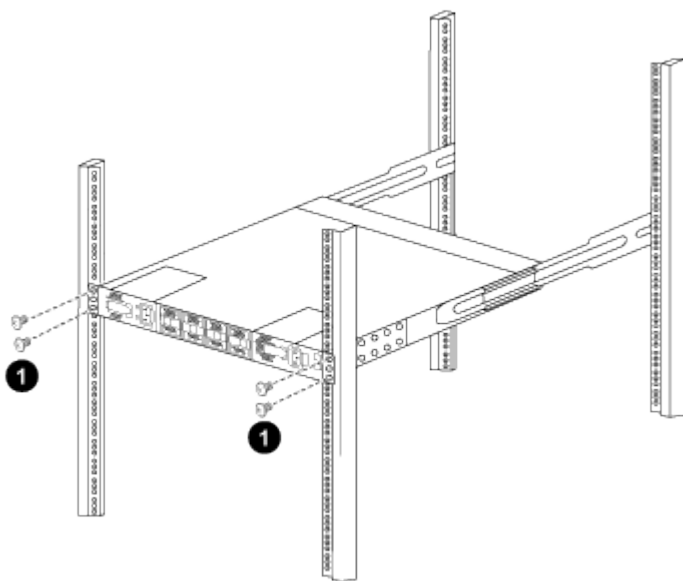
- a. Posizionare la parte posteriore dell'interruttore su RU41.



(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.

5. Una volta installati gli interruttori, collegare i cavi di collegamento alle prese di alimentazione degli interruttori.

6. 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.

7. Collegare la porta di gestione su ogni switch 3232C 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 3232C, leggere le seguenti considerazioni.

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

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

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

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

Configurare il software

Flusso di lavoro di installazione del software per gli switch cluster Cisco Nexus 3232C

Per installare e configurare il software per uno switch Cisco Nexus 3232C e installare o aggiornare il file di configurazione di riferimento (RCF), attenersi alla seguente procedura:

1

"Configurare l'interruttore"

Configurare lo switch cluster 3232C.

2

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

Il software Cisco NX-OS e i file di configurazione di riferimento (RCF) devono essere installati sugli switch cluster Cisco 3232C.

3

"Installa o aggiorna il software NX-OS"

Scaricare e installare o aggiornare il software NX-OS sullo switch cluster Cisco 3232C.

4

"Installare l'RCF"

Installare l'RCF dopo aver configurato per la prima volta lo switch Cisco 3232C.

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 3232C.

Configurare lo switch cluster 3232C

Seguire questa procedura per impostare e configurare lo switch Cisco Nexus 3232C.

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 la rete cluster e per lo switch di rete di gestione.

Vedere ["Documentazione richiesta"](#) per maggiori informazioni.

- Documentazione richiesta del controller e documentazione ONTAP .

["Documentazione NetApp"](#)

- Licenze applicabili, informazioni di rete e configurazione e cavi.
- Schede di lavoro sui cablaggi completate.
- 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 3232C 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 3232C e di un pannello pass-through in un cabinet NetApp .
Apparecchiature in un rack Telco	Consultare le procedure fornite nelle guide all'installazione dell'hardware dello switch e nelle istruzioni di installazione e configurazione NetApp .

2. Cablare la rete del cluster e gli switch della rete di gestione ai controller utilizzando i fogli di lavoro di cablaggio compilati.
3. Accendere la rete del cluster e gli switch e i controller della rete di gestione.
4. Eseguire una configurazione iniziale degli switch di rete del cluster.

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

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

Richiesta	Risposta
Configurare la stringa di comunità SNMP di sola lettura? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Configurare la stringa di comunità SNMP di lettura-scrittura? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Inserisci il nome dello switch.	Il nome dello switch è limitato a 63 caratteri alfanumerici.
Continuare con la configurazione della gestione fuori banda (mgmt0)? (sì/no)	Rispondere con sì (impostazione predefinita) a tale richiesta. Al prompt mgmt0 IPv4 address:, inserisci il tuo indirizzo IP: ip_address.
Configurare il gateway predefinito? (sì/no)	Rispondi con sì . All'indirizzo IPv4 del prompt default-gateway:, immettere default_gateway.
Configurare le opzioni IP avanzate? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Abilitare il servizio telnet? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Servizio SSH abilitato? (sì/no)	<p>Rispondi con sì. L'impostazione predefinita è sì.</p> <div>  <p>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.</p> </div>
Inserisci il tipo di chiave SSH che vuoi generare (dsa/rsa/rsa1).	Il valore predefinito è rsa .
Inserire il numero di bit della chiave (1024-2048).	Inserisci il numero di bit della chiave da 1024 a 2048.
Configurare il server NTP? (sì/no)	Rispondi con no . L'impostazione predefinita è no.
Configurare il livello di interfaccia predefinito (L3/L2):	Rispondi con L2 . Il valore predefinito è L2.
Configura lo stato predefinito dell'interfaccia della porta dello switch (shut/noshut):	Rispondi con noshut . L'impostazione predefinita è noshut.
Configurare il profilo del sistema CoPP (rigoroso/moderato/indulgente/de nso):	Rispondi con rigoroso . L'impostazione predefinita è rigorosa.

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

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

Cosa succederà ora?

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

Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento (RCF)

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.

Nomenclatura di switch e nodi

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=x h`

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



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

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

```
set -privilege advanced
```

Il prompt avanzato(*>) appare.

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

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
cluster1-02/cdp			
	e0a	cs1	Eth1/2
C3232C			
	e0b	cs2	Eth1/2
C3232C			
cluster1-01/cdp			
	e0a	cs1	Eth1/1
C3232C			
	e0b	cs2	Eth1/1
C3232C			

4 entries were displayed.

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

a. Visualizza gli attributi della porta di rete:

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

Mostra esempio

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

```
Node: cluster1-02
```

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

```
Node: cluster1-01
```

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

```
4 entries were displayed.
```

a. Visualizza informazioni sui LIF: `network interface show -vserver Cluster`

Mostra esempio

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

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

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

4 entries were displayed.

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		

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

Tutte le versioni ONTAP

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

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

```

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

```

1. Verificare che il auto-revert il comando è abilitato su tutti i LIF del cluster: network interface show -vserver Cluster -fields auto-revert

Mostra esempio

```

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

```

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

4 entries were displayed.

Cosa succederà ora?

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

Installa il software NX-OS

È possibile utilizzare questa procedura per installare il software NX-OS sullo switch cluster Nexus 3232C.

Requisiti di revisione

Prima di iniziare

- Un backup attuale della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- ["Pagina dello 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 , fare riferimento alle guide software e di aggiornamento appropriate disponibili sul sito Web Cisco .

Installa il software

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 di NX-OS e RCF"](#) 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

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

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

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

3. 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-
C3232C
          e0d    cs2                Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3232C
          e0d    cs2                Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3232C
          e0b    cs2                Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3232C
          e0b    cs2                Ethernet1/1/2    N3K-
C3232C
cluster1::*>
```

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

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

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

Mostra esempio

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

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

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

Mostra esempio

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

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

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

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

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

Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.90      N3K-
C3232C
    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-
C3232C
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

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

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

6. Copiare il software NX-OS e le immagini EPLD sullo switch Nexus 3232C.

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.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.4.img /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGD

  Device name: cs2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 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          v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(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
```

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

Software
  BIOS: version 08.37
  NXOS: version 9.3(4)
  BIOS compile time: 01/28/2020
  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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
Reason: Reset due to upgrade
```

```
System version: 9.3(3)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

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

Mostra esempio

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

EPLD Device	Version
MI FPGA	0x12
IO FPGA	0x11

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	Disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x12	0x12	No
1	SUP	IO FPGA	0x11	0x12	Yes

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

Module 1 EPLD upgrade is successful.

```
cs2#
```

11. Se si esegue l'aggiornamento alla versione NX-OS 9.3(11), è necessario aggiornare l'EPLD golden immagine e riavviare nuovamente lo switch. Altrimenti, passare al passaggio 12.

Vedere ["Note di rilascio dell'aggiornamento EPLD, versione 9.3\(11\)"](#) per ulteriori dettagli.

Mostra esempio

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable      Impact          Reason
-----
-----
          1          SUP          Yes          Disruptive      Module
Upgradable

Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : MI FPGA [Programming] : 100.00% (      64 of      64 sect)
Module 1 : IO FPGA [Programming] : 100.00% (      64 of      64 sect)
Module 1 EPLD upgrade is successful.
Module          Type          Upgrade-Result
-----
-----
          1          SUP          Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#
```

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

Mostra esempio

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

EPLD Device	Version
MI FPGA	0x12
IO FPGA	0x12

13. 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
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
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					

Node: cluster1-04

Ignore

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

8 entries were displayed.

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

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-01/cdp	e0a	cs1	Ethernet1/7	N3K-
C3232C	e0d	cs2	Ethernet1/7	N3K-
C3232C				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N3K-
C3232C	e0d	cs2	Ethernet1/8	N3K-
C3232C				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N3K-
C3232C	e0b	cs2	Ethernet1/1/1	N3K-
C3232C				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N3K-
C3232C	e0b	cs2	Ethernet1/1/2	N3K-
C3232C				

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

Switch Model	Type	Address	
cs1	cluster-network	10.233.205.90	N3K-
C3232C			
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-

```

C3232C
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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

```

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

```

14. 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::*>

```

15. Ripetere i passaggi da 6 a 14 sullo switch cs1.

16. Abilita il ripristino automatico sui LIF del cluster.

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

17. 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 3232C, 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 3232C. 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
Archiviazione 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 panoramica della 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 3232C, 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.

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

Fase 1: installare l'RCF sugli switch

1. Accedi per cambiare cs2 tramite SSH o tramite una console seriale.
2. 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"](#) .

Mostra esempio

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Applicare l'RCF precedentemente scaricato al bootflash.

Per ulteriori informazioni sui comandi Cisco , consultare la guida appropriata nel ["Riferimento ai comandi](#)

Mostra esempio

Questo esempio mostra il file RCF `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` in fase di installazione sullo switch `cs2`:

```
cs2# copy Nexus_3232C_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.

4. Esaminare l'output del banner dal `show banner motd` comando. È necessario leggere e seguire le istruzioni riportate nella sezione **Note importanti** per garantire la corretta configurazione e il corretto funzionamento dello switch.
5. Verificare che il file RCF sia la versione più recente corretta:

```
show running-config
```

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

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

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

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



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

```
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
```

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

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
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.

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

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

10. 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
```

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

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

12. Riavviare lo switch cs2:

```
cs2# reload
```

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

13. Ripetere i passaggi da 1 a 12 sullo switch cs1.

14. 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 -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 LIFS del cluster non sono tornati alle loro porte home, ripristinarli manualmente: `network interface revert -vserver <vserver_name> -lif <lif_name>`

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
4 entries were displayed.
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-
C3232C
              e0d    cs2                      Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
              e0a    cs1                      Ethernet1/8      N3K-
C3232C
              e0d    cs2                      Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
              e0a    cs1                      Ethernet1/1/1    N3K-
C3232C
              e0b    cs2                      Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N3K-
C3232C
              e0b    cs2                      Ethernet1/1/2    N3K-
C3232C
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 -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        Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
          cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01 e0a      true
          cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01 e0d      true
          cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02 e0a      true
          cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02 e0d      true
          cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03 e0a      true
          cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03 e0b      true
          cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04 e0a      true
          cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04 e0b      true
8 entries were displayed.
cluster1::*>

```

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

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

Mostra esempio

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.92
NX3232C
    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     10.233.205.93
NX3232C
    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.
```

3. Disabilitare il ripristino automatico sui LIF del cluster.

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

Passaggio 2: configurare le porte

1. Sullo switch del cluster 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
```



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

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

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

Mostra esempio

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

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

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

3. Verificare che il cluster sia integro:

```
cluster show
```

Mostra esempio

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

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

```
show running-config
```

5. Registrare eventuali aggiunte personalizzate tra l'attuale running-config e il file RCF in uso (ad esempio una configurazione SNMP per la tua organizzazione).
6. Salva i dettagli di configurazione di base nel write_erase.cfg file sul bootflash.



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

```
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 racl-lite 512" >>
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:

```
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

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_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

Questo esempio mostra il file RCF `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` in fase di installazione sullo switch cs2:

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands
```



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

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

```
show running-config
```

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

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

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

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

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

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

18. Riavviare lo switch cs2. È possibile ignorare gli eventi "porte cluster inattive" segnalati sui nodi mentre lo switch si riavvia.

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

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

a. Verificare che le porte e0d 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
```

Speed (Mbps)

```

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

```

- b. Verificare lo stato di integrità dello switch dal cluster (potrebbe non essere visualizzato lo switch cs2, poiché i LIF non sono posizionati su e0d).

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-C3232C
          e0d      cs2                      Ethernet1/7
N3K-C3232C
cluster01-2/cdp
          e0a      cs1                      Ethernet1/8
N3K-C3232C
          e0d      cs2                      Ethernet1/8
N3K-C3232C
cluster01-3/cdp
          e0a      cs1                      Ethernet1/1/1
N3K-C3232C
          e0b      cs2                      Ethernet1/1/1
N3K-C3232C
cluster1-04/cdp
          e0a      cs1                      Ethernet1/1/2
N3K-C3232C
          e0b      cs2                      Ethernet1/1/2
N3K-C3232C
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
cs1                                     cluster-network      10.233.205.90
N3K-C3232C
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                9.3(4)
    Version Source: CDP
cs2                                     cluster-network      10.233.205.91
N3K-C3232C
    Serial Number: FOXXXXXXXXGS
```

```
Is Monitored: true
Reason: None
Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
9.3(4)
Version Source: CDP
2 entries were displayed.
```



A seconda della versione RCF precedentemente caricata sullo switch, è possibile che venga visualizzato il seguente output sulla console dello switch cs1: 17 nov 2020 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT: Sblocco della porta port-channel1 su VLAN0092. Coerenza della porta ripristinata. 17 nov 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Blocco del port-channel1 su VLAN0001. Peer VLAN incoerente. 17 nov 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Blocco del port-channel1 su VLAN0092. VLAN locale incoerente.



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

L'esempio seguente utilizza l'output dell'esempio di interfaccia del passaggio 1:

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

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

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

Mostra esempio

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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		
8 entries were displayed.				
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 4 a 19 sullo switch cs1.

24. Abilita il ripristino automatico sui LIF del cluster.

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

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

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

```
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 -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 LIFS del cluster non sono tornati alle loro porte home, ripristinarli manualmente: `network interface revert -vserver vserver_name -lif lif_name`

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

4 entries were displayed.

```
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 `show` comando per visualizzare i dettagli.

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

Packet		Source	Destination
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			
.			
.			
cluster1-03			
.			
.			
.			
.			
cluster1-04			
.			
.			
.			
.			

Tutte le versioni ONTAP

Per tutte le versioni ONTAP , è anche possibile utilizzare `cluster ping-cluster -node <name>`

comando per verificare la connettività: `cluster ping-cluster -node <name>`

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

Cosa succederà ora?

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

Verifica la tua configurazione SSH

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

Passi

1. Verificare che SSH sia abilitato:

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

2. Verificare che le chiavi SSH siano abilitate:

```
show ssh key
```

Mostra esempio

```
(switch)# show ssh key

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

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

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

could not retrieve dsa key information

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

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

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

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



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

Cosa succederà ora?

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

Ripristinare lo switch del cluster 3232C ai valori predefiniti di fabbrica

Per ripristinare le impostazioni predefinite di fabbrica dello switch cluster 3232C, è necessario cancellare le impostazioni dello switch 3232C.

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 switchless a due nodi

Migrazione da un flusso di lavoro cluster switchless a due nodi

Seguire questi passaggi del flusso di lavoro per migrare da un cluster switchless a due nodi a un cluster con switch cluster Cisco Nexus 3232C.

1

"Requisiti di migrazione"

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

2

"Prepararsi alla migrazione"

Prepara il tuo cluster switchless a due nodi per la migrazione a un cluster switched a due nodi.

3

"Configura le tue porte"

Configura il tuo cluster switchless a due nodi per la migrazione a un cluster switched a due nodi.

4

"Completa la tua migrazione"

Completa la migrazione a un cluster commutato a due nodi.

Requisiti di migrazione

Se si dispone di un cluster switchless a due nodi, è possibile migrare a un cluster switch a due nodi che include switch di rete cluster Cisco Nexus 3232C. Si tratta di una procedura non distruttiva.

Prima di iniziare

Verificare le seguenti installazioni e connessioni:

- Sono disponibili porte per le connessioni dei nodi. Gli switch cluster utilizzano le porte Inter-Switch Link (ISL) e1/31-32.
- Si dispone di cavi adatti per le connessioni del cluster:
 - 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 40/100 GbE richiedono moduli ottici QSFP/QSFP28 supportati con cavi in fibra o cavi di collegamento diretto in rame QSFP/QSFP28.
 - Gli switch del cluster richiedono il cablaggio ISL appropriato:
 - 2 cavi QSFP28 in fibra o rame a collegamento diretto.
- Le configurazioni sono impostate correttamente e funzionano.

I due nodi devono essere connessi e funzionare in un ambiente cluster senza switch a due nodi.

- Tutte le porte del cluster sono nello stato **attivo**.
- Sono supportati gli switch cluster Cisco Nexus 3232C.
- La configurazione di rete del cluster esistente è la seguente:
 - Un'infrastruttura cluster Nexus 3232C ridondante e completamente funzionale su entrambi gli switch
 - Le ultime versioni RCF e NX-OS sui tuoi switch
 - Connettività di gestione su entrambi gli switch
 - Accesso alla console per entrambi gli switch
 - Tutte le interfacce logiche del cluster (LIF) nello stato **attivo** senza essere state migrate
 - Personalizzazione iniziale dello switch
 - Tutte le porte ISL abilitate e cablate

Informazioni sugli esempi utilizzati

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

- Switch cluster Nexus 3232C, **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 "[Universo Hardware](#)" contiene dettagli sulle porte del cluster sulle tue piattaforme.

- **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 del cluster **C2** per il nodo **n2**.
- Il numero di porte 10 GbE e 40/100 GbE è definito nei file di configurazione di riferimento (RCF) disponibili sul "[Download del file di configurazione di riferimento dello switch di rete Cisco® Cluster](#)" pagina.



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

Prepararsi alla migrazione da cluster switchless a due nodi a cluster switched a due nodi

Seguire questi passaggi per preparare il cluster switchless a due nodi alla migrazione a un cluster switch a due nodi che include switch di rete cluster Cisco Nexus 3232C.

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 -role cluster
```


Mostra esempio

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

Ignore

Health      Health      Speed (Mbps)
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      Health      Speed (Mbps)
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 e sui nodi home designati:

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

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.
```

- c. Verificare che il rilevamento del cluster senza switch sia abilitato utilizzando il comando con privilegi avanzati:

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

Mostra esempio

L'output nell'esempio seguente mostra che il rilevamento del cluster senza switch è abilitato:

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

3. Verificare che sui nuovi switch 3232C siano installati gli RCF e l'immagine appropriati ed effettuare le personalizzazioni necessarie al sito, ad esempio aggiungendo utenti, password e indirizzi di rete.

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:

- a. Vai alla pagina *Switch Ethernet Cisco* sul sito di supporto NetApp .

["Switch Ethernet Cisco"](#)

- b. Annota il tuo switch e le versioni software richieste nella tabella in quella pagina.

- c. Scarica la versione appropriata di RCF.
- d. Selezionare **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.

["Download del file di configurazione di riferimento per Cisco Cluster and Management Network Switch"](#)

4. Selezionare **CONTINUA** nella pagina **Descrizione**, accettare il contratto di licenza e quindi seguire le istruzioni nella pagina **Download** per scaricare l'RCF.
5. Sugli switch Nexus 3232C C1 e C2, disabilitare tutte le porte C1 e C2 rivolte al nodo, ma non disabilitare le porte ISL e1/31-32.

Per ulteriori informazioni sui comandi Cisco , vedere l'elenco seguente in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

L'esempio seguente mostra le porte da 1 a 30 disabilite sugli switch cluster Nexus 3232C C1 e C2 utilizzando una configurazione supportata in RCF NX3232_RCF_v1.0_24p10g_24p100g.txt :

```
C1# copy running-config startup-config
[] 100% 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
[] 100% 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
```

6. Collegare le porte 1/31 e 1/32 su C1 alle stesse porte su C2 utilizzando il cablaggio supportato.
7. Verificare che le porte ISL siano operative su C1 e C2:

```
show port-channel summary
```

Per ulteriori informazioni sui comandi Cisco , vedere l'elenco seguente in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

L'esempio seguente mostra Cisco show port-channel summary comando utilizzato per verificare che le porte ISL siano operative su C1 e C2:

```
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

-----
-----
      Port-
Group Channel          Type   Protocol  Member Ports
-----
-----
1      Po1(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-           Type   Protocol  Member Ports
      Channel
-----
-----
1      Po1(SU)         Eth    LACP      Eth1/31(P)  Eth1/32(P)
```

8. Visualizza l'elenco dei dispositivi adiacenti sullo switch.

Per ulteriori informazioni sui comandi Cisco , vedere l'elenco seguente in "[Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000](#)".

Mostra esempio

L'esempio seguente mostra il comando Cisco `show cdp neighbors` utilizzato per visualizzare i dispositivi vicini sullo switch:

```
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-C3232C
Eth1/31
C2                  Eth1/32       174    R S I s          N3K-C3232C
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-C3232C
Eth1/31
C1                  Eth1/32       178    R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
```

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

```
network device-discovery show
```

Mostra esempio

L'esempio seguente mostra la connettività delle porte del cluster visualizzata per 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

Cosa succederà ora?

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

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

Seguire questi passaggi per configurare le porte per la migrazione da un cluster switchless a due nodi a un cluster switch a due nodi su switch Nexus 3232C.

Passi

1. Migrare i LIF n1_clus1 e n2_clus1 alle porte fisiche dei loro nodi di destinazione:

```
network interface migrate -vserver vservice-name -lif lif-name source-node  
source-node-name -destination-port destination-port-name
```

Mostra esempio

È necessario eseguire il comando per ciascun nodo locale come mostrato nell'esempio seguente:

```
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
```

2. Verificare che le interfacce del cluster siano state migrate correttamente:

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

Mostra esempio

L'esempio seguente mostra che lo stato "Is Home" per i LIF n1_clus1 e n2_clus1 è diventato "false" dopo il completamento della migrazione:

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
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.
```

3. Arrestare le porte del cluster per i LIF n1_clus1 e n2_clus1, migrati nel passaggio 9:

```
network port modify -node node-name -port port-name -up-admin false
```

Mostra esempio

È necessario eseguire il comando per ogni porta come mostrato nell'esempio seguente:

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

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

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>
```



```

cluster1::*> cluster ping-cluster -node local
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 9000 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. Scollegare 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 per gli switch Nexus 3232C.

2. Scollegare 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.

Per ulteriori informazioni sui comandi Cisco , consultare le guide elencate in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

L'esempio seguente mostra le porte da 1 a 30 abilitate sugli switch cluster Nexus 3232C C1 e C2 utilizzando la configurazione supportata in RCF NX3232_RCF_v1.0_24p10g_26p100g.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 -node node-name -port port-name -up-admin true
```

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 -role cluster
```

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.
```

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

```
network interface revert -vserver cluster -lif lif-name
```

Mostra esempio

È necessario ripristinare ogni LIF alla propria porta di origine singolarmente, come mostrato nell'esempio seguente:

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

7. Verificare che tutti i LIF siano ora ripristinati alle loro porte di origine:

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

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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a n1_clus1 up/up 10.10.0.1/24 n1
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-C3232C
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	n1	e4e	FAS9000

9. Migrare clus2 sulla porta e4a sulla console di ciascun nodo:

```
network interface migrate cluster -lif lif-name -source-node source-node-name  
-destination-node destination-node-name -destination-port destination-port-  
name
```

Mostra esempio

È necessario migrare ogni LIF alla sua porta home individualmente, come mostrato nell'esempio seguente:

```
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
```

Mostra esempio

L'esempio seguente mostra le porte specificate impostate su `false`, chiudendo le porte 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
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4a      false
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4a      false
4 entries were displayed.
```

12. Scollegare 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 sul nodo n1, utilizzando il cablaggio appropriato per il modello di switch Nexus 3232C.

13. Scollegare 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 appropriato per il modello di switch Nexus 3232C.

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 NX3232C_RCF_v1.0_24p10g_26p100g.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
```

Mostra esempio

L'esempio seguente mostra la seconda porta del cluster e4e attivata su ciascun nodo:

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

16. 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_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

Cosa succederà ora?

Dopo aver configurato le porte, puoi [completare la tua migrazione](#) .

Completa la migrazione da un cluster switchless a due nodi a un cluster switched a due nodi

Completare i seguenti passaggi per finalizzare la migrazione del cluster switchless a due nodi in un cluster switchato a due nodi su switch Nexus 3232C.

Passi

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

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

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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a n1_clus1 up/up 10.10.0.1/24 n1
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.
```

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

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

3. Visualizza i numeri delle porte dello switch del cluster tramite cui ogni porta del cluster è connessa a ciascun nodo:

```
network device-discovery show
```


Mostra esempio

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

4. Visualizza gli switch del cluster rilevati e monitorati:

```
system cluster-switch show
```

Mostra esempio

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

Switch Model	Type	Address
C1 NX3232CV Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP	cluster-network	10.10.1.101
C2 NX3232CV Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP	cluster-network	10.10.1.102

2 entries were displayed.

5. Verificare che il rilevamento del cluster senza switch abbia modificato l'opzione del cluster senza switch in disabilitata:

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

6. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

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>
```

```

cluster1::*> cluster ping-cluster -node local
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 9000 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

Sostituire uno switch cluster Cisco Nexus 3232C

Per sostituire uno switch Cisco Nexus 3232C difettoso in un cluster, seguire questi passaggi. Si tratta di una procedura non distruttiva.

Requisiti di revisione

Cosa ti servirà

Assicurarsi che la configurazione di rete e del cluster esistente abbia le seguenti caratteristiche:

- L'infrastruttura del cluster Nexus 3232C è ridondante e completamente funzionale su entrambi gli switch.

Nella pagina relativa agli switch Ethernet Cisco sono disponibili le versioni RCF e NX-OS più recenti sui tuoi switch.

- Tutte le porte del cluster devono essere nello stato **attivo**.
- La connettività di gestione deve essere presente su entrambi gli switch.
- Tutte le interfacce logiche del cluster (LIF) sono nello stato **attivo** e non vengono migrate.

Lo switch sostitutivo Cisco Nexus 3232C presenta le seguenti caratteristiche:

- La connettività della rete di gestione è funzionale.
- L'accesso alla console per l'interruttore sostitutivo è pronto.
- L'immagine appropriata del sistema operativo RCF e NX-OS viene caricata sullo switch.
- La personalizzazione iniziale dello switch è completa.

Per maggiori informazioni

Vedere quanto segue:

- ["Switch Ethernet Cisco"](#)
- ["Hardware Universe"](#)
- ["Quali informazioni aggiuntive mi servono per installare la mia attrezzatura che non è presente in HWU?"](#)

Abilita la registrazione della console

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

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

Sostituire l'interruttore

Informazioni su questo compito

Questa procedura di sostituzione descrive il seguente scenario:

- Inizialmente il cluster è composto da quattro nodi collegati a due switch cluster Nexus 3232C, CL1 e CL2.
- Si prevede di sostituire lo switch cluster CL2 con C2 (passaggi da 1 a 21):
 - Su ciascun nodo, si migrano i LIF del cluster connessi allo switch del cluster CL2 alle porte del cluster connesse allo switch del cluster CL1.
 - Scollegare il cablaggio da tutte le porte sullo switch cluster CL2 e ricollegarlo alle stesse porte sullo switch cluster sostitutivo C2.
 - Ripristinare i LIF del cluster migrati su ciascun nodo.

Informazioni sugli esempi

Questa procedura di sostituzione sostituisce il secondo switch cluster Nexus 3232C CL2 con il nuovo switch 3232C C2.

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

- I quattro nodi sono n1, n2, n3 e n4.
- 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 40/100 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 esempi in questa procedura di sostituzione utilizzano quattro nodi. Due dei 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 verificare le porte del cluster corrette per la tua piattaforma.

Passaggio 1: visualizzare e migrare le porte del cluster per passare

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
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3232C
	e0b	CL2	Ethernet1/1/1	N3K-C3232C
	e0c	CL2	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
	e0c	CL2	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
	e4e	CL2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3232C
	e4e	CL2	Ethernet1/8	N3K-C3232C

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

a. Visualizza gli attributi della porta di rete:

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

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

```

b. Visualizza informazioni sulle interfacce logiche (LIF):

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

Mostra esempio

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

	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			

c. Visualizza gli switch del cluster rilevati:

```
system cluster-switch show
```

Mostra esempio

Il seguente esempio di output visualizza gli switch del cluster:

```
cluster::> system cluster-switch show
Switch                                Type                                Address
Model
-----
CL1                                  cluster-network                    10.10.1.101
NX3232C
    Serial Number: FOX000001
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version 7.0(3)I6(1)
    Version Source: CDP

CL2                                  cluster-network                    10.10.1.102
NX3232C
    Serial Number: FOX000002
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version 7.0(3)I6(1)
    Version Source: CDP
```

4. Verificare che sul nuovo switch Nexus 3232C siano installati l'RCF e l'immagine appropriati ed effettuare le personalizzazioni del sito necessarie.

- a. Vai al sito di supporto NetApp .

["mysupport.netapp.com"](https://mysupport.netapp.com)

- b. Andare alla pagina **Switch Ethernet Cisco ** e annotare le versioni software richieste nella tabella.

["Switch Ethernet Cisco"](#)

- c. Scarica la versione appropriata dell'RCF.

- d. Fare clic su **CONTINUA** nella pagina **Descrizione**, accettare il contratto di licenza e quindi andare alla pagina **Download**.

- e. Scaricare la versione corretta del software di immagine dalla pagina ** Download del file di configurazione di riferimento dello switch di rete Cisco® Cluster and Management**.

["Download del file di configurazione di riferimento per Cisco® Cluster and Management Network Switch"](#)

5. Migrare i LIF del cluster alle porte del nodo fisico connesse allo switch sostitutivo C2:

```
network interface migrate -vserver vserver-name -lif lif-name -source-node
node-name -destination-node node-name -destination-port port-name
```

Mostra esempio

È necessario migrare singolarmente tutti i LIF del cluster, come mostrato nell'esempio seguente:

```
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. Verificare lo stato delle porte del cluster e le loro designazioni home:

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

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
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			

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

```
network port modify -node node-name -port port-name -up-admin false
```

Mostra esempio

L'esempio seguente mostra che le porte di interconnessione del cluster sono disattivate 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 `show` comando per visualizzare i dettagli.

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

Packet			Source	Destination
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>
```

```

cluster1::*> cluster ping-cluster -node local
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 9000 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)
```

Fase 2: Migrare gli ISL per passare a CL1 e C2

1. Disattivare le porte 1/31 e 1/32 sullo switch cluster CL1.

Per ulteriori informazioni sui comandi Cisco , consultare le guide elencate in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

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

2. Rimuovere tutti i cavi collegati allo switch del cluster CL2 e ricollegarli allo switch sostitutivo C2 per tutti i nodi.
3. Rimuovere i cavi di collegamento inter-switch (ISL) dalle porte e1/31 ed e1/32 sullo switch del cluster CL2 e ricollegarli alle stesse porte sullo switch sostitutivo C2.
4. Attivare le porte ISL 1/31 e 1/32 sullo switch cluster CL1.

Per ulteriori informazioni sui comandi Cisco , consultare le guide elencate in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

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

5. Verificare che gli ISL siano attivi su CL1.

Per ulteriori informazioni sui comandi Cisco , consultare le guide elencate in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

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)
```

6. Verificare che gli ISL siano attivi sullo switch del cluster C2.

Per ulteriori informazioni sui comandi Cisco , consultare le guide elencate in ["Riferimenti ai comandi NX-OS della serie Cisco Nexus 3000"](#) .

Mostra esempio

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

```
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
Channel
-----
-----
1      Po1 (SU)      Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

7. Su tutti i nodi, richiamare tutte le porte di interconnessione del cluster connesse allo switch sostitutivo C2:

```
network port modify -node node-name -port port-name -up-admin true
```

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
```

Passaggio 3: ripristinare tutti i LIF alle porte originariamente assegnate

1. Ripristina tutti i LIF di interconnessione del cluster migrati su tutti i nodi:

```
network interface revert -vserver cluster -lif lif-name
```

Mostra esempio

È necessario ripristinare singolarmente tutti i LIF di interconnessione del cluster, come mostrato nell'esempio seguente:

```
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
```

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

```
network interface show
```

Mostra esempio

L'esempio seguente 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 una porta ha un valore di 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			

3. Verificare che le porte del cluster siano connesse:

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

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

Speed (Mbps) Health

Health

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

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

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

-

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

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>
```



```

cluster1::*> cluster ping-cluster -node local
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 9000 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 4: verificare che tutte le porte e LIF siano migrati correttamente

1. Visualizza le informazioni sui dispositivi nella tua configurazione immettendo i seguenti comandi:

È possibile eseguire i seguenti comandi in qualsiasi ordine:

- ° 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	Interface	Platform
-----	-----	-----	-----	-----
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

```
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

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	

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

Node: n4

Ignore

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

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

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

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

Cluster					
	nm1_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			

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

Switch	Type	Address
Model		
-----	-----	-----
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2	cluster-network	10.10.1.102
NX3232C		
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2	cluster-network	10.10.1.103
NX3232C		
Serial Number: FOX000003		

```
Is Monitored: true
```

```
Reason: None
```

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

```
Software, Version 7.0(3)I6(1)
```

```
Version Source: CDP 3 entries were displayed.
```

2. Eliminare lo switch cluster sostituito CL2 se non è stato rimosso automaticamente:

```
system cluster-switch delete -device cluster-switch-name
```

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

```
system cluster-switch show
```

Mostra esempio

L'esempio seguente mostra che gli switch del cluster vengono monitorati perché Is Monitored lo stato è true .

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

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

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

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

Cosa succederà ora?

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

Sostituisci gli switch cluster Cisco Nexus 3232C con connessioni switchless

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

Requisiti di revisione

Linee guida

Rivedere le seguenti linee guida:

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

Prima di iniziare

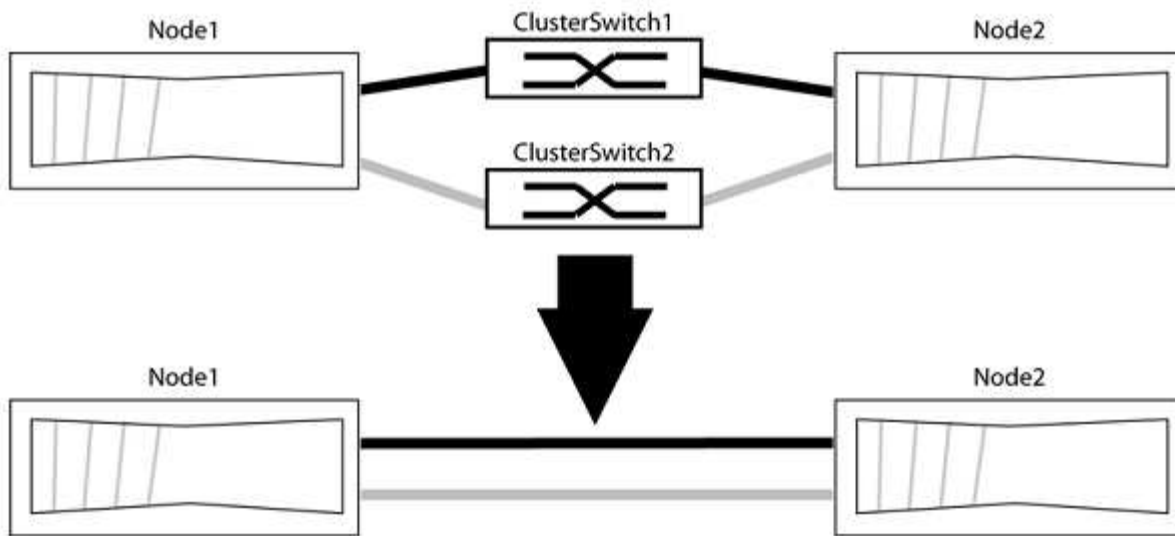
Assicurati di avere quanto segue:

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

Migrare gli switch

Informazioni su questo compito

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



Informazioni sugli esempi

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

Fase 1: Prepararsi alla migrazione

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

```
set -privilege advanced
```

Il prompt avanzato `*>` appare.

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

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

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

Mostra esempio

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

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

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

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


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

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

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

Mostra esempio

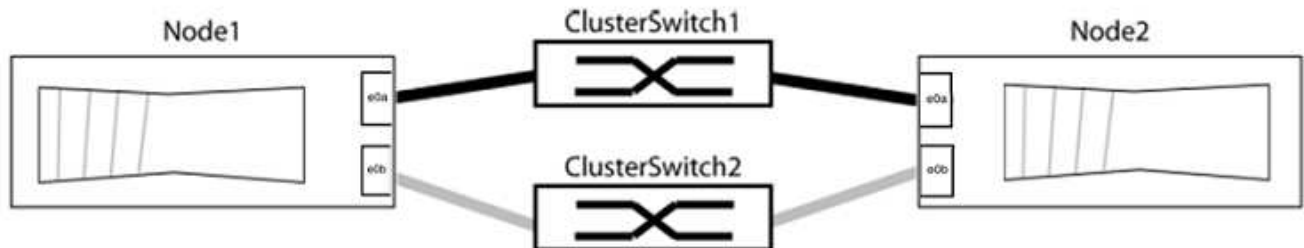
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Passaggio 2: configurare porte e cablaggio

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

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

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



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

Mostra esempio

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

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

Node: node2

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

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

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

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

Mostra esempio

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

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

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

4. Disabilitare il ripristino automatico per i LIF del cluster:

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

5. Verificare che tutte le porte elencate nel passaggio precedente siano connesse a uno switch di rete:

```
network device-discovery show -port cluster_port
```

La colonna "Dispositivo rilevato" dovrebbe contenere il nome dello switch del cluster a cui è connessa la porta.

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono collegate correttamente agli switch del cluster "cs1" e "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Tutte le versioni ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verificare che il cluster sia integro:

```
cluster ring show
```

Tutte le unità devono essere master o secondarie.

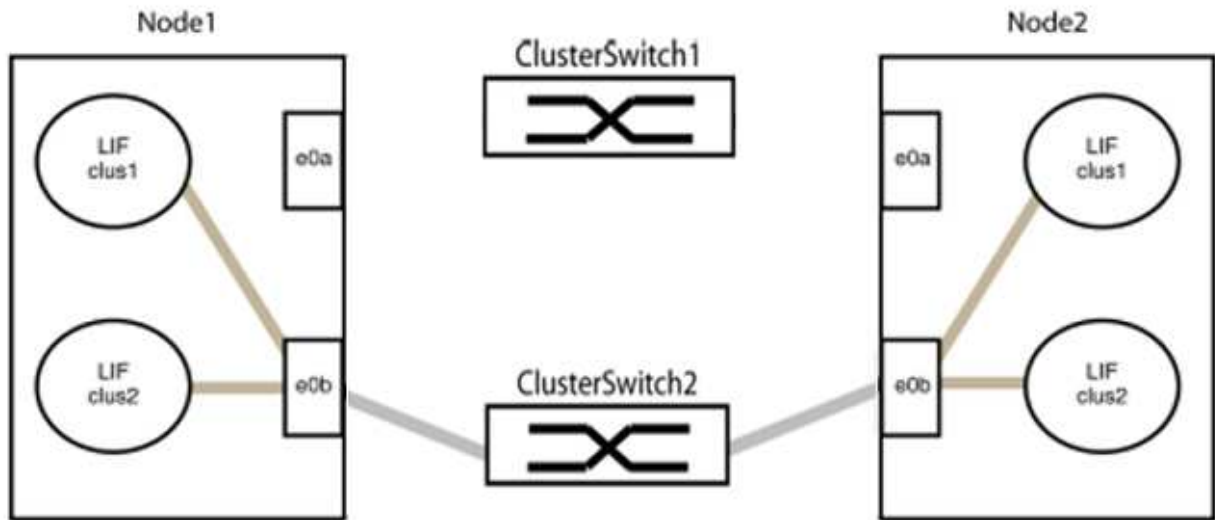
2. Impostare la configurazione senza switch per le porte del gruppo 1.



Per evitare potenziali problemi di rete, è necessario scollegare le porte dal gruppo 1 e ricollegarle una dopo l'altra il più rapidamente possibile, ad esempio **in meno di 20 secondi**.

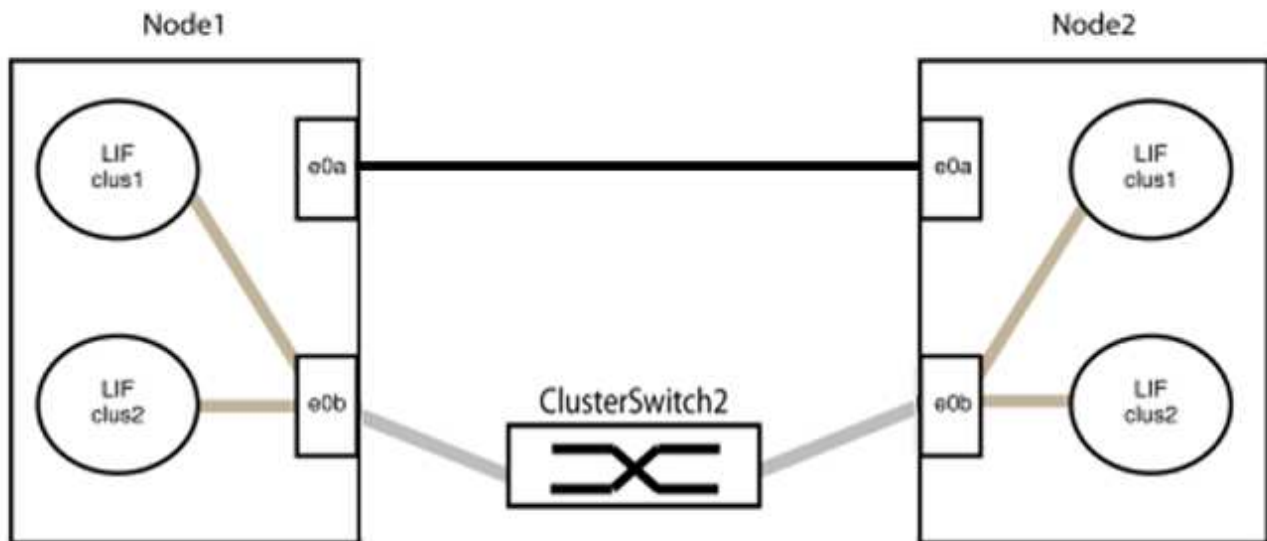
- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 1.

Nell'esempio seguente, i cavi vengono scollegati dalla porta "e0a" su ciascun nodo e il traffico del cluster continua attraverso lo switch e la porta "e0b" su ciascun nodo:



b. Collegare le porte del gruppo 1 una dietro l'altra.

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



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

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

L'esempio seguente mostra che il cluster switchless è abilitato:

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

4. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node1			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Tutte le versioni ONTAP

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

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



```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```



Prima di procedere al passaggio successivo, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

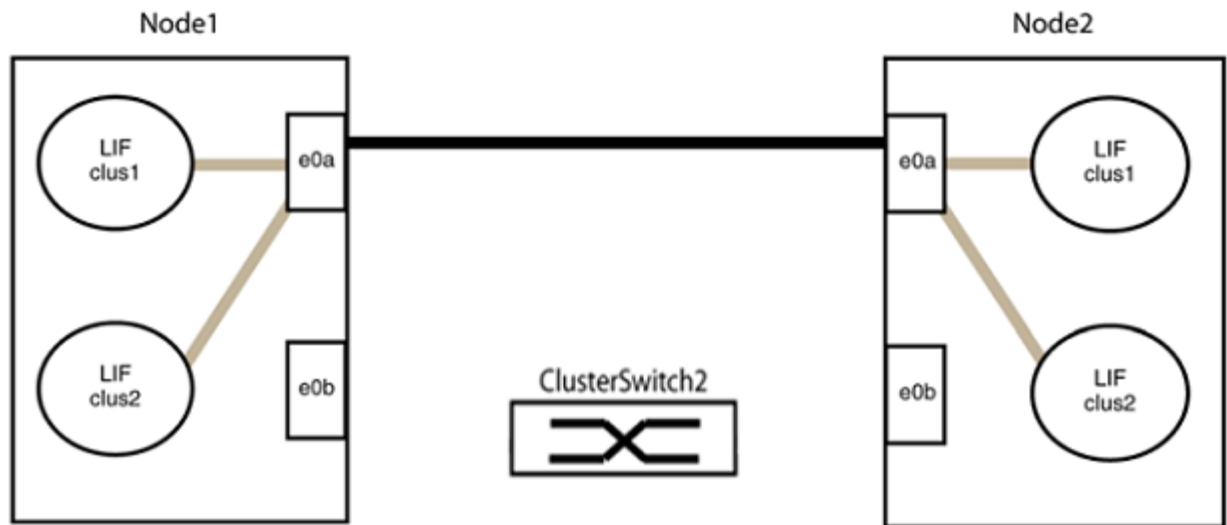
1. Impostare la configurazione senza switch per le porte nel gruppo 2.



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

- a. Scollegare contemporaneamente tutti i cavi dalle porte del gruppo 2.

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



b. Cablare le porte del gruppo 2 una dietro l'altra.

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



Passaggio 3: verificare la configurazione

1. Verificare che le porte su entrambi i nodi siano collegate correttamente:

```
network device-discovery show -port cluster_port
```

Mostra esempio

L'esempio seguente mostra che le porte del cluster "e0a" e "e0b" sono correttamente collegate alla porta corrispondente sul partner del cluster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a    node2                      e0a        AFF-A300
           e0b    node2                      e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                      e0a        AFF-A300
           e0b    node1                      e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Riattivare il ripristino automatico per i LIF del cluster:

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

3. Verificare che tutti i LIF siano a casa. Potrebbero volerci alcuni secondi.

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

Mostra esempio

I LIF sono stati ripristinati se la colonna "È a casa" è true , come mostrato per node1_clus2 E node2_clus2 nell'esempio seguente:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Se uno qualsiasi dei LIFS del cluster non è tornato alle proprie porte home, ripristinarlo manualmente dal nodo locale:

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

4. Controllare lo stato del cluster dei nodi dalla console di sistema di uno dei due nodi:

```
cluster show
```

Mostra esempio

L'esempio seguente mostra epsilon su entrambi i nodi da false :

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Verificare la connettività delle interfacce del cluster remoto:

ONTAP 9.9.1 e versioni successive

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

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

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

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

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

Tutte le versioni ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. 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
```

Switch di archiviazione Cisco 3232C

Sostituire uno switch di archiviazione Cisco Nexus 3232C

Per sostituire uno switch di archiviazione Cisco Nexus 3232C difettoso, seguire questi passaggi. Si tratta di una procedura non distruttiva.

Requisiti di revisione

La configurazione di rete esistente deve avere le seguenti caratteristiche:

- Nella pagina relativa agli switch Ethernet Cisco sono disponibili le versioni RCF e NX-OS più recenti sui tuoi switch.
- La connettività di gestione deve essere presente su entrambi gli switch.



Assicurati di aver completato tutti i passaggi per la risoluzione dei problemi per confermare che il tuo switch debba essere sostituito.

Lo switch sostitutivo Cisco Nexus 3232C deve avere le seguenti caratteristiche:

- La connettività della rete di gestione deve essere funzionale.
- Deve essere presente l'accesso alla console per l'interruttore sostitutivo.
- Sullo switch deve essere caricata l'immagine appropriata del sistema operativo RCF e NX-OS.
- La personalizzazione iniziale dello switch deve essere completa.

Sostituire l'interruttore

Questa procedura sostituisce il secondo switch di archiviazione Nexus 3232C S2 con il nuovo switch 3232C NS2. I due nodi sono node1 e node2.

Passaggio 1: confermare che l'interruttore da sostituire è S2

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. Controllare lo stato di integrità delle porte del nodo di archiviazione per assicurarsi che vi sia una connessione allo switch di archiviazione S1:

```
storage port show -port-type ENET
```

Mostra esempio

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed	State	Status	VLAN
				(Gb/s)			ID

node1	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

3. Verificare che lo switch di archiviazione S1 sia disponibile:

```
network device-discovery show
```


Mostra esempio

```
storage::*> network device-discovery show
```

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

node1/cdp				
	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700				
node1/lldp				
	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
node2/cdp				
	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700				
node2/lldp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-

4. Esegui il `show lldp neighbors` comando sullo switch funzionante per confermare che puoi vedere entrambi i nodi e tutti gli scaffali:

```
show lldp neighbors
```

Mostra esempio

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID                Local Intf          Hold-time  Capability  Port
ID
node1                    Eth1/1             121        S           e3a
node2                    Eth1/2             121        S           e3a
SHFGD2008000011          Eth1/5             121        S           e0a
SHFGD2008000011          Eth1/6             120        S           e0a
SHFGD2008000022          Eth1/7             120        S           e0a
SHFGD2008000022          Eth1/8             120        S           e0a
```

Passaggio 2: configurare il cablaggio

1. Verificare le porte dello scaffale nel sistema di archiviazione:

```
storage shelf port show -fields remote-device,remote-port
```

Mostra esempio

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
----- --  -
3.20   0   Ethernet1/5  S1
3.20   1   -            -
3.20   2   Ethernet1/6  S1
3.20   3   -            -
3.30   0   Ethernet1/7  S1
3.20   1   -            -
3.30   2   Ethernet1/8  S1
3.20   3   -            -
```

2. Rimuovere tutti i cavi collegati all'interruttore di archiviazione S2.
3. Ricollegare tutti i cavi allo switch sostitutivo NS2.

Passaggio 3: verificare tutte le configurazioni dei dispositivi sullo switch NS2

1. Verificare lo stato di integrità delle porte del nodo di archiviazione:

storage port show -port-type ENET

Mostra esempio

```
storage::*> storage port show -port-type ENET
```

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						

node1						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online
node2						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online
30						

2. Verificare che entrambi gli switch siano disponibili:

network device-discovery show

Mostra esempio

```
storage::*> network device-discovery show
```

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

node1/cdp				
	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700	e7b	NS2	Ethernet1/1	
NX3232C				
node1/lldp				
	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
	e7b	NS2	Ethernet1/1	-
node2/cdp				
	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700	e7b	NS2	Ethernet1/2	
NX3232C				
node2/lldp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-
	e7b	NS2	Ethernet1/2	-

3. Verificare le porte degli scaffali nel sistema di archiviazione:

```
storage shelf port show -fields remote-device,remote-port
```

Mostra esempio

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf id remote-port remote-device  
-----  
3.20 0 Ethernet1/5 S1  
3.20 1 Ethernet1/5 NS2  
3.20 2 Ethernet1/6 S1  
3.20 3 Ethernet1/6 NS2  
3.30 0 Ethernet1/7 S1  
3.20 1 Ethernet1/7 NS2  
3.30 2 Ethernet1/8 S1  
3.20 3 Ethernet1/8 NS2
```

4. 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?

"Configurare il monitoraggio dello stato dello switch"

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.